Quantum Information Techniques for Quantum Metrology

Nathan Shettell

Quantum Information Techniques for Quantum Metrology

Nathan Shettell

Laboratoire d'Informatique de Paris 6

SORBONNE UNIVERSITÉ

Jacob Dunningham, *Professeur, University of Sussex, Angleterre*	Rapporteur
Pieter Kok, *Professeur, University of Sheffield, Angleterre*	Rapporteur
Lorenzo Maccone, *Professeur, Università di Pavia, Italie*	Examinateur
Nicolas Treps, *Professeur, Sorbonne Université, France*	Examinateur
Pérola Milman, *Directrice de recherche, CNRS, France*	Examinateur
Damian Markham, *Chargé de recherche, CNRS, France*	Directeur de Thèse

Submitted for the degree of

Doctor of Philosophy

DECEMBER 2021

Try and be nice to people, avoid eating fat, read a good book every now and then, get some walking in, and try and live together in peace and harmony with people of all creeds and nations.

-Monty Python's The Meaning of Life

Abstract (English)

Quantum metrology is an auspicious discipline of quantum information which is currently witnessing a surge of experimental breakthroughs and theoretical developments. The main goal of quantum metrology is to estimate unknown parameters as accurately as possible. By using quantum resources as probes, it is possible to attain a measurement precision that would be otherwise impossible using the best classical strategies. For example, with respect to the task of phase estimation, the maximum precision (the Heisenberg limit) is a quadratic gain in precision with respect to the best classical strategies. Of course, quantum metrology is not the sole quantum technology currently undergoing advances. The theme of this thesis is exploring how quantum metrology can be enhanced with other quantum techniques when appropriate, namely: graph states, error correction and cryptography.

Graph states are an incredibly useful and versatile resource in quantum information. We aid in determining the full extent of the applicability of graph states by quantifying their practicality for the quantum metrology task of phase estimation. In particular, the utility of a graph state can be characterised in terms of the shape of the corresponding graph. From this, we devise a method to transform any graph state into a larger graph state (named a bundled graph state) which approximately saturates the Heisenberg limit. Additionally, we show that graph states are a robust resource against the effects of noise, namely dephasing and a small number of erasures, and that the quantum Cramér-Rao bound can be saturated with a simple measurement strategy.

Noise is one of the biggest obstacles for quantum metrology that limits its achievable precision and sensitivity. It has been showed that if the environmental noise is distinguishable from the dynamics of the quantum metrology task, then frequent applications of error correction can be used to combat the effects of noise. In practise however, the required frequency of error correction to maintain Heisenberg-like precision is unobtainable for current quantum technologies. We explore the limitations of error correction enhanced quantum metrology by taking into consideration technological constraints and impediments, from which, we establish the regime in which the Heisenberg limit can be maintained in the presence of noise.

Fully implementing a quantum metrology problem is technologically demanding: entangled quantum states must be generated and measured with high fidelity. One solution, in the instance where one lacks all of the necessary quantum hardware, is to delegate a task to a third party. In doing so, several security issues naturally arise because of the possibility of interference of a malicious adversary. We address

these issues by developing the notion of a cryptographic framework for quantum metrology. We show that the precision of the quantum metrology problem can be directly related to the soundness of an employed cryptographic protocol. Additionally, we develop cryptographic protocols for a variety of cryptographically motivated settings, namely: quantum metrology over an unsecured quantum channel and quantum metrology with a task delegated to an untrusted party.

Quantum sensing networks have been gaining interest in the quantum metrology community over the past few years. They are a natural choice for spatially distributed problems and multiparameter problems. The three proposed techniques, graph states, error correction and cryptography, are a natural fit to be immersed in quantum sensing network. Graph states are an well-known candidate for the description of a quantum network, error correction can be used to mitigate the effects of a noisy quantum channel, and the cryptographic framework of quantum metrology can be used to add a sense of security. Combining these works formally is a future perspective.

Résumé (Français)

La métrologie quantique est une discipline prometteuse de l'information quantique qui connaît actuellement une vague de percées expérimentales et de développements théoriques. L'objectif principal de la métrologie quantique est d'estimer des paramètres inconnus aussi précisément que possible. En utilisant des ressources quantiques comme sondes, il est possible d'atteindre une précision de mesure qui serait autrement impossible en utilisant les meilleures stratégies classiques. Par exemple, en ce qui concerne la tâche d'estimation de la phase, la précision maximale (la limite d'Heisenberg) est un gain de précision quadratique par rapport aux meilleures stratégies classiques. Bien entendu, la métrologie quantique n'est pas la seule technologie quantique qui connaît actuellement des avancées. Le thème de cette thèse est l'exploration de la manière dont la métrologie quantique peut être améliorée par d'autres techniques quantiques lorsque cela est approprié, à savoir : les états graphiques, la correction d'erreurs et la cryptographie.

Les états de graphes sont une ressource incroyablement utile et polyvalente dans l'information quantique. Nous aidons à déterminer l'étendue de l'applicabilité des états de graphes en quantifiant leur utilité pour la tâche de métrologie quantique de l'estimation de phase. En particulier, l'utilité d'un état de graphe peut être caractérisée en fonction de la forme du graphe correspondant. À partir de là, nous concevons une méthode pour transformer tout état de graphe en un état de graphe plus grand (appelé "bundled graph states") qui sature approximativement la limite de Heisenberg. En outre, nous montrons que les états de graphe constituent une ressource robuste contre les effets du bruit (le déphasage et un petit nombre d'effacements) et que la limite quantique de Cramér-Rao peut être saturée par une simple stratégie de mesure.

Le bruit issu de l'environnement est l'un des principaux obstacles à la métrologie quantique, qui limite la précision et la sensibilité qu'elle peut atteindre. Il a été démontré que si le bruit environnemental peut être distingué de la dynamique de la tâche de métrologie quantique, des applications fréquentes de correction d'erreurs peuvent être utilisées pour combattre les effets du bruit. En pratique, cependant, la fréquence de correction d'erreurs requise pour maintenir une précision de type Heisenberg est impossible à atteindre pour les technologies quantiques actuelles. Nous explorons les limites de la métrologie quantique améliorée par la correction d'erreurs en prenant en compte les contraintes et les obstacles technologiques, à partir desquels nous établissons le régime dans lequel la limite d'Heisenberg peut être maintenue en présence de bruit.

La mise en œuvre complète d'un problème de métrologie quantique est technologiquement exigeante : des états quantiques intriqués doivent être générés et mesurés avec une grande fidélité. Une solution, dans le cas où l'on ne dispose pas de tout le matériel quantique nécessaire, consiste à déléguer une tâche à un tiers. Ce faisant, plusieurs problèmes de sécurité se posent naturellement en raison de la possibilité d'interférence d'un adversaire malveillant. Nous abordons ces questions en développant la notion de cadre cryptographique pour la métrologie quantique. Nous montrons que la précision du problème de la métrologie quantique peut être directement liée à la solidité d'un protocole cryptographique employé. En outre, nous développons des protocoles cryptographiques pour une variété de paramètres motivés par la cryptographie, à savoir : la métrologie quantique sur un canal quantique non sécurisé et la métrologie quantique avec une tâche déléguée à une partie non fiable.

Les réseaux de détection quantique ont suscité un intérêt croissant dans la communauté de la métrologie quantique au cours des dernières années. Ils constituent un choix naturel pour les problèmes distribués dans l'espace et les problèmes multiparamètres. Les trois techniques proposées, les états de graphes, la correction d'erreurs et la cryptographie, s'intègrent naturellement dans les réseaux de détection quantique. Les états de graphes sont un candidat bien connu pour la description d'un réseau quantique, la correction d'erreurs peut être utilisée pour atténuer les effets d'un canal quantique bruyant et le cadre cryptographique de la métrologie quantique peut être utilisé pour ajouter un sentiment de sécurité. La combinaison formelle de ces travaux est une perspective future.

List Of Publications

In Publication

- N. Shettell and D. Markham, "Graph states as a resource for quantum metrology", *Physical Review Letters*, vol. 124, no. 11, p. 110 502, 2020.
- N. Shettell, W. J. Munro, D. Markham, and K. Nemoto, "Practical limits of error correction for quantum metrology", *New Journal of Physics*, vol. 23, no. 4, p. 043 038, 2021.
- Y. Ouyang, N. Shettell, and D. Markham, "Robust quantum metrology with explicit symmetric states", *IEEE Transactions on Information Theory*, 2021.

Pre-Print

- N. Shettell, D. Markham, and E. Kashefi, "A cryptographic approach to quantum metrology", *arXiv preprint arXiv:2101.01762*, 2021.

In Preparation

- N. Shettell and D. Markham, "Quantum Metrology with Delegated Tasks".

Acknowledgements

The beauty of physics lies within its impossibly large scope. To paraphrase french philosopher Maupertuis: 'the movement of animals and the vegetative growth of plants are consequences of the laws of nature'. These laws nature which govern a physical system take into account innate properties, but also interactions with other systems. The liminal space that is a PhD is not subjected to the aforementioned laws of nature, yet, there is an analogous statement to be made about my PhD journey, in that it was molded by properties of my own self, like passion and persistence, but also, the interactions I had with others. Before delving into the contents of this thesis, I would like to extend my gratitude to those who helped shape the last three years of my life into such a rich and fulfilling experience.

First and foremost, I would like to thank my supervisor Damian for his support and flexibility. The environment fostered by Damian is a perfect balance of guidance and freedom. I am extremely grateful for his insights and perspectives. For the opportunity to work in Tokyo for six months. For instigating Friday night beers. For being an exemplary researcher.

Thanks to my friends and colleagues of LIP6. The colourful cast of characters made for an entertaining work environment, which, as far as I'm concerned, is unparalleled. Thank you for the coffee breaks. Thank you for the post-work trips to the bar. Thank you for the insightful academic discussions and the delightful balderdash. Good luck to all for great beginnings.

Thanks to those at NII and to those at Sakura house in Tabata. My time spent in Japan was unforgettable: the remarkable food, overnight karaoke and the magical countryside. ありがとうございました。 I would like to thank Prof. Kae Nemoto and Dr. Bill Munro, for taking on an unofficial role of co-supervisors while I was present. Thank you for the mentorship and guidance, and for integrating me in your group. I thoroughly enjoyed my time at NII.

Thank you to my friends at the Maison des étudiants canadiens. Thank you for reminding me of home, the shenanigans on the terrace, Wednesday night karaoke at Fleurus, and the Sunday brunches. Specifically, for those present during restrictions brought on by the pandemic of Covid-19: la confinement, couvrefeu, fermeture des bars et restaurants, ou peu importe. Thank you for the sense of community.

Last, but by no means the least, thank you to my family: Mom, Dad, Brit and Jake. I am grateful for the unconditional love and support from across the Atlantic. Without you, I would not be the person I am today.

Per aspera ad astra.

Table of Contents

1 Introduction

1.1 Quantum Technologies

The advent of quantum theory has completely revolutionized modern physics. The underlying dynamics are perplexing and counter intuitive - e.g. depending on the circumstance, electrons exhibit wave-like or particle-like behaviour [DG28] - and has since changed our perspective of the universe at the microscopic level.

> *Those who are not shocked when they first come across quantum theory cannot possibly have understood it.*
>
> -Niels Bohr

Erwin Schrödinger received a Nobel prize in 1933 for his work establishing the basis of quantum mechanics and atomic theory. Be that as it may, nearly twenty years later in 1953, he begins a lecture in Dublin with a humorous forewarning that the contents of the lecture may seem 'lunatic' [Bit96]. Clearly said in jest, there is inherent truth in this statement. Quantum theory allows for dynamics which are not observed at the macroscopic level, and as a result are difficult to envisage. The most prominent of which are: entanglement and superposition. *Quantum entanglement* is a term coined to indicate non-classical correlations between quantum systems. When a single constituent of an entangled quantum system is measured, the effects propagate amongst the complete system. *Quantum superposition* is the principle that any configuration of superposed quantum states is also an allowable quantum state.

The first theoretical prototypes of quantum computers were pioneered in the 1980's [Ben80; Fey82; Deu85]; this was the beginning of the quantum information

zeitgeist. Such a computer would be compromised of microscopic objects subjected to the realm of quantum mechanics. In particular, a two level quantum system, such as the spin of an electron, is characterized as a quantum version of the traditional binary bit - usually abbreviated to *qubit*. By virtue of quantum mechanical effects, such as entanglement and superposition, a quantum computer can greatly outperform the abilities of a classical (i.e. inherently *not*-quantum) computer [Pre12]. For example, Shor's algorithm (an algorithm designed to be carried out on quantum computers) can find the prime factorization of large numbers in a small amount of time [Sho94]; a task which is extremely difficult for the world's most state of the art supercomputer. In 2019, Google demonstrated that their 53 qubit quantum computer could execute a sampling task in 200 seconds [Aru+19]. Even though IBM showed that this task could be executed by a classical computer in two and a half days [Ped+19], it quickly converges to an impossible problem for a classical computer as the number of qubits increase incrementally. Practically, we are entering the era where classical computers cannot compete.

Quantum computing is not the unique technology proposed as an advantageous version of its classical analogue. For the past few decades, academic and government institutions, and even some companies such as Google and IBM, have increased their investment and support in the quest of designing quantum technologies [DM03]. In China, satellites are being used for long distance quantum key distribution [Lia+17]. In Europe, a rudimentary version of a quantum internet is in development [Kim08; WEH18]. Quantum technologies are often divided into four categories depending on their scope: quantum computation, quantum simulation, quantum communication, and quantum metrology and sensing [Ací+18]. The focal point of this thesis is quantum metrology and sensing technologies enhanced by other quantum information techniques, namely graph states (computation and communication), quantum error correction (computation) and quantum cryptography (communication).

Quantum metrology and sensing is a relatively new and auspicious type of quantum technology [Par09; TA14; DRC17], in which quantum phenomena are exploited to accurately estimate physical parameters with a precision which cannot matched with the best classical strategies [Cav81]. Since the publication of *Quantum-enhanced measurements: beating the standard quantum limit* [GLM04] by Giovannetti, Lloyd and Maccone, there has been a surge of interest in the field. Current research is flourishing at a theoretical and experimental level.

1.2 Metrology: From Classical To Quantum

Metrology, the science of measurement and precision, is often not discussed and regularly misunderstood as meteorology (the science of weather). Be that as it may, metrology plays a critical role in the advancement of science. Scientific theories are tested by observing a physical processes predicted by said theory; in physics and chemistry this step is often carried out by performing a measurement. As the accuracy of technology improves, more theories are put to the test. In 2016, LIGO (in collaboration with VIRGO) announced successful observations of gravitational waves[1][2] [Abb+16], a phenomenon predicted by Einstein's theory of general relativity. In 2021, the standard model for particle physics was put under scrutiny after Fermilab released their measurement results of the anomalous magnetic dipole moment of the muon [Abi+21], in which the measured value was different than the predicted value by the current theory. In a similar vein to its importance to science, metrology is an unsung hero of engineering, architecture and design. A chair/table/house/bridge in which the lengths are measured up to the nearest tenth of millimeter is more reliable and safe than a counterpart in which the lengths are measured up to the nearest centimeter.

Alas, most physical parameters of interest cannot be associated with a direct measurement process. A more accurate description is to say such a parameter is *estimated*. The underlying tool of constructing an estimate is still a measurement of a related (measurable) quantity. In the LIGO experiment, the gravitational wave introduced a relative phase in the light source. A relative phase is not a directly measurable quantity, instead the phase was estimated from the observed interference pattern. Formally, *estimation theory* is the branch of statistics which establishes techniques and the mathematical formalism pertaining to estimating unknown parameters from measured empirical data [Kay93; Cox06]. It is the principal mathematics of metrology.

There are two major philosophies of estimation theory: the Bayesian approach and the frequentist approach. The Bayesian approach is used for stochastic parameters and the frequentist approach is used for deterministic parameters. This thesis

[1] The experiment is currently being upgraded to use squeezed light which will allow for an even more accurate measurement [Aas+13].

[2] A Michelson interferometer with arms which spanned four kilometers in length was used in the experiment, and the achieved precision was comparable to measuring the distance from Earth to the nearest star (besides the sun) with an uncertainty smaller than the width of a human hair [LIG17].

focuses uniquely on the frequentist approach to quantum metrology[3]. With sufficient measurement data, the frequency of observations will begin to mimic the true probability distribution, hence the name 'frequentist'. In principle, a deterministic parameter can be estimated to any degree of precision with a sufficiently large set of empirical data. The precision of an estimate is denoted by the mean-squared error. Within the frequentist framework, this is ultimately bounded by the reciprocal of the Fisher information - a measure of how much information the measurable data contains about the unknown data [Fis25; Kul97]. This bound is called the Cramér-Rao bound [Cra46; Rad45].

Estimation theory was formally adapted to realm of quantum information in the latter half of the 20th century by Helstrom [Hel67; Hel68; Hel69] and Holevo [Hol73; Hol82]. The established terminology to describe quantum parameter estimation is difficult to misconstrue; as the rhetorical tradition dictates, existing terminology is preceded by the word *quantum*, for example *quantum Cramér-Rao bound*, *quantum Fisher information*, et cetera [BC94; Hay05]. In quantum parameter estimation problems, an unknown parameter is encoded into a quantum probe by a physical interaction. As a result of quantum phenomena, quantum parameter estimation problems can attain a precision impossible to a purely classical system [Cav81; BS84]. An experimental quantum advantage has been reported using optical systems [Oka+08; Kac+10; Xia+11], atomic systems [Mey+01; Tay+08; Fac+16; Cha+18; Die+19] and superconducting circuits [Wan+19].

Phase estimation is the canonical problem of quantum metrology [HB93; GLM04; TA14]. An unknown phase is encoded in an n qubit highly entangled GHZ state, and a simple measurement strategy can be implemented to estimate the unknown phase such that the mean squared error scales as $1/n^2$. This notion of precision (where the quantum Cramér-Rao bound is saturated) is referred to as the *Heisenberg limit*: the ultimate limit of precision enabled by quantum mechanics [GLM06]. With respect to phase estimation, the Heisenberg limit is a quadratic advantage over the analogous scenario sans non-classical correlations (i.e. the n qubits are not entangled). Here the mean-squared error is dictated by the central limit theorem and scales as $1/n$, this notion of precision is commonly referred to as the *standard quantum limit*, classical limit or the shot-noise limit.

The applicability of quantum metrology spans a number of domains. These include, but are not limited to, magnetometry [Tay+08; Was+10; Sew+12; BCK15; Raz+19], thermometry [Neu+13; Toy+13; Cor+15], gravimetry [Qva+18; Kri+18], spectroscopy [Mey+01; Lei+04; Kir+11; DSM16; Sha+18], imaging [LGB02; Bar+15;

[3] A summary of Bayesian estimation theory is provided in **Chapter 3** for completeness.

Gen16] and clock synchronization [GLM01; App+09; Lud+15; Sch+17]. Quantum metrology is particularly appealing for biology and medicine [Peñ+12; Sch+14; TB16; MO18], where probing a sample is often destructive in nature, and so the non-classical correlations of quantum systems may lead to a reduction in the number of probes required whilst still attaining a required precision.

1.3 Motivation

The overarching theme of this thesis is the incorporation of other quantum information techniques within the usual quantum metrology framework. Specifically, we explore the immersion of graph states [SM20], quantum error correction [She+21], and quantum cryptography [SMK21; SM]. All of these technologies offer a unique functionality to the standard quantum metrology problem with respect to different circumstances.

Firstly, in the case of graph states, having an multi-purposeful resource is very desirable for the realm of quantum technologies, as focusing on a specific class of quantum states will greatly facilitate the design and implementation of quantum hardware. Graph states [HEB04] come to mind as a potential 'super resource', as they are used for many tasks in quantum computation [SW01; RBB03] and quantum communication [MS08; MMG19; HPE19]. In this context then, it is a natural question to ask which graph states are an efficient resource for quantum metrology [SM20].

Secondly, we consider the utility of error correction. One of the biggest obstacles for early generations quantum hardware will be its susceptibility to quantum noise. It is known that said noise imposes many challenge for quantum metrology [EdMD11a; EdMD11b; DKG12; KD13]. It has been shown that quantum error correction can be used to completely mitigate the effects of noise [DCS17; Zho+18]. Unfortunately, the necessary frequency of error correction is impossible for current quantum hardware [Cra+16; Ofe+16]. Thus, it is important to determine the utility of quantum error correction in a real world scenario [She+21].

Finally, we consider a cryptographic framework. Another obstacle for the early generations of quantum hardware is the lack of 'all-in-one' devices. Because quantum metrology is technologically demanding, one solution is to delegate some of the difficult tasks to a third party with more computational power. In this event, quantum information will have to be transmitted through a quantum channel. This raises several security issues, as quantum channels can be intercepted by malicious

adversaries. It is critical to properly adapt the parameter estimation problem in such a cryptographic setting as many of the standard assumptions, namely having an unbiased estimator, may not necessarily be true [SMK21]. An equally important task is to create cryptographic protocols which do not interfere with the underlying quantum metrology problem, but provide a sense of privacy and security [SMK21; SM].

Formally, multiple parties communicating through a quantum channel is known as a quantum network [CDP09]. Quantum networks have been proposed as a resource for spatially separated quantum metrology and multiparameter quantum metrology [Kóm+14; Kóm+16; Eld+18; Ge+18; PKD18; ZZS18; Qia+19; Rub+20; Guo+20]. The quantum technologies discussed in this thesis (graph states, error correction and cryptography) all fit in naturally within the framework of quantum networks. A future perspective is to combine these works in interesting and useful ways. Currently, we are combining the cryptographically themed results to establish a notion of a secure quantum sensing network.

1.4 Thesis Outline

The subsequent chapters of this thesis are partitioned into two preliminary chapters, three research chapters and a discussion chapter. The research chapters provide insight on the projects I worked on during my PhD in a pedagogical fashion. Following the main chapters are three appendices, which contain proofs omitted from the main text due to length or complexity.

The preliminary chapters equip the reader with the necessary definitions and mathematical tools to comprehend the subsequent research chapters. **Chapter 2** acts a crash course on the mathematics of quantum mechanics specific to quantum information. Key concepts such as quantum states, entanglement and quantum measurements are explained. **Chapter 3** overviews the foundations of the parameter estimation problem and its adaptation to the realm of quantum information. The canonical example of a highly entangled quantum state used for phase estimation is explored in this chapter and it is regularly used as a comparison in the research chapters.

Chapter 4 is based on the work *Graph states as a resource for quantum metrology* [SM20]. We characterize the use of graph states for quantum metrology by linking the quantum Fisher information to the shape of the corresponding graph. We construct a class of graph states which approximately achieve the Heisenberg

limit for phase estimation and are thus a practical resource for quantum metrology. We name this class of graph states bundled graph states, as many vertices in the corresponding graph are in bundles which are permutation invariant. We also show that the Heisenberg limit can maintain a quantum advantage in the presence of noise and that the Cramér-Rao bound can be saturated with a simple measurement strategy.

Chapter 5 is based on the work *Practical limits of error correction for quantum metrology* [She+21]. We analyze the effectiveness of a realistic quantum error correction scheme to mitigate the impact of noise for quantum metrology. This is accomplished by incorporating impediments an implementation of an error correction code may face, such as a delay in any error correction operations, noisy ancillary qubits and imperfect operations. We outline the circumstances in which the Heisenberg limit may be recovered. Even though this work focuses on a specific error correction code (the parity check code), we hypothesize that other error correction strategies encounter the same limitations.

Chapter 6 is based on the work *A Cryptographic approach to Quantum Metrology* [SMK21] as well as *Quantum Metrology with Delegated Tasks* [SM]. We provide a rigorous framework of the functionality of quantum metrology problems in a cryptographically motivated setting. By integrating an appropriate cryptographic protocol, the functionality of the parameter estimation scheme is mostly unchanged. We show that the added bias and additional uncertainty in the cryptographic framework can be bounded in terms of the soundness of the protocol. We establish protocols for a variety of possible settings, such as exchanging information over an unsecured quantum channel [SMK21], and delegating a portion of the quantum metrology scheme to an untrusted party [SM].

Chapter 7 is a discussion chapter; the key ideas from the main research chapters are summarized and future perspectives are listed. Insight on a current project is given, where the core concept is an amalgamation of quantum networks and the cryptographic framework for quantum metrology to devise a notion of a secure quantum sensing network.

2 Mathematical Foundations of Quantum Information

Quantum theory is an extensive area of physics with a rich mathematical history. The majority of its subtleties are beyond the scope of this thesis. This chapter is intended to familiarize the reader with the underlying mathematics of the subsequent chapters. See [GS18] for a broader overview of quantum mechanics, and [NC02] for a more detailed analysis of quantum information.

> *As Deepak Chopra taught us, quantum physics means anything can happen at any time for no reason!*
>
> -Professor Farnsworth

2.1 Quantum States

2.1.1 Qubits

The bit is the primitive building block of information theory. It can be thought of as a physical switch, or any object subjected to a binary state: 0 or 1, yes or no, on or off, et cetera. The quantum bit, commonly referred to as a qubit, is the analogous primitive building block of *quantum information*. Just as a bit can be in the states 0 and 1, a qubit can be in the states $|0\rangle$ and $|1\rangle$[1]. Unlike a classical bit, the state of

[1] The notation $|\square\rangle$, known as Dirac notation or bra-ket notation, is ubiquitously used in quantum mechanics to describe quantum states.

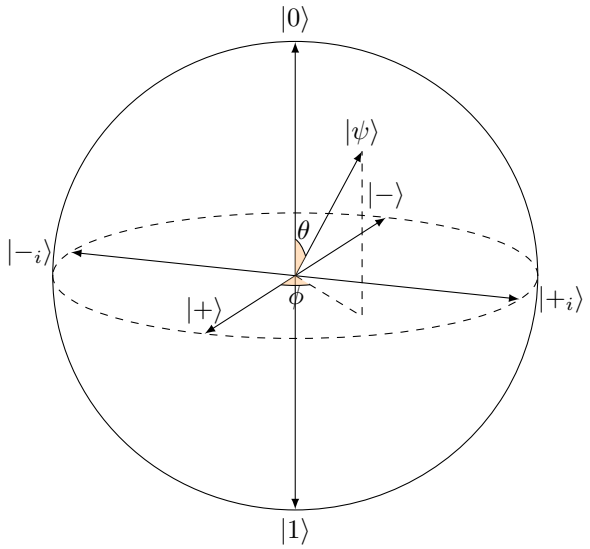


Figure 2.1: The Bloch sphere is a geometric representation of single qubit quantum states. A point on the surface of the sphere with polar angle θ and azimuthal angle ϕ represents the quantum state $|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle$.

a qubit can be any linear combination of $|0\rangle$ and $|1\rangle$:

$$\alpha\,|0\rangle + \beta\,|1\rangle \tag{2.1}$$

with α and β being complex numbers subjected to $|\alpha|^2 + |\beta|^2 = 1$. This is the *superposition principle*, which asserts that any linear combination of valid quantum states is also a valid quantum state.

Just as a bit can be thought of as a physical object, so can a qubit. There exists a variety of physical implementations to realize a qubit, for example, the spin of an electron [Chi+06; Dut+07], the direction of current in a superconducting circuit [Wen17] or the polarization of a photon [Str+07]. Having said that, in this thesis (unless it is otherwise stated) a quantum state should be thought of as a mathematical element of a Hilbert space $\mathcal{H}$, formally one writes $|\psi\rangle \in \mathcal{H}$. For a qubit, $\mathcal{H}$ is a two dimensional space, hence $\{|0\rangle, |1\rangle\}$ corresponds to an orthonormal basis. This is not the sole basis representation for qubits; other commonly used bases are $\{|+\rangle, |-\rangle\}$, where $|\pm\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle \pm |1\rangle\big)$ and $\{|+_i\rangle, |-_i\rangle\}$, where $|\pm_i\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle \pm i\,|1\rangle\big)$. For any orthonormal basis $\{|x\rangle, |y\rangle\}$, the inner product of quantum states $|\psi\rangle = \alpha\,|x\rangle + \beta\,|y\rangle$ and $|\phi\rangle = \gamma\,|x\rangle + \delta\,|y\rangle$ is defined to be

$$\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^* = \alpha\gamma^* + \beta\delta^*, \tag{2.2}$$

where an asterisk is used to signify the complex conjugate.

The 2-dimensional Hilbert space of a qubit naturally generalizes to d-dimensional spaces. These quantum states are commonly known as *qudits* and can be represented via

$$\sum_{k=0}^{d-1} \alpha_k \left|k\right\rangle , \tag{2.3}$$

where $\sum_{k=0}^{d-1} |\alpha_k|^2 = 1$ and $\{|0\rangle, \ldots, |d-1\rangle\}$ forms a basis for said Hilbert space. Even though the results presented throughout this thesis are derived with respect to systems composed of qubits, the techniques presented (quantum metrology, graph states, error correction and cryptography) have higher dimensional forms, and thus the results presented can be generalized to systems composed of qudits.

2.1.2 Multiple Qubits And Quantum Entanglement

A bipartite quantum system composed of $|\psi_A\rangle \in \mathcal{H}_A$ and $|\psi_B\rangle \in \mathcal{H}_B$ is represented via

$$|\psi_{AB}\rangle = |\psi_A\rangle |\psi_B\rangle \in \mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B. \tag{2.4}$$

The above quantum states are called *separable*, as the composite system is (by construction) a product of quantum states each belonging to a separate Hilbert space. By the superposition principle, the composite Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ also contains superpositions of separable quantum states. The two-qubit quantum state

$$\frac{1}{\sqrt{2}}\left(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B \right) \tag{2.5}$$

cannot be written as a product of two one-qubit quantum states. In other words, each qubit in the composite system cannot be described independently from one another. This property is better known as *entanglement* and is a peculiarity unique to quantum mechanics. Quantum entanglement is the root of the well-known (and frequently misinterpreted in popular media[2]) Schrödinger's thought experiment [Sch35]. In the thought experiment, a hypothetical cat is placed in a box with a radioactive source and a flask of poison. The poison is released upon detecting that the radioactive source has decayed: killing the cat. The premise is that the nature of the cat is entangled with the radioactive source. When the state of the source evolves to a superposition of 'not-decayed' and 'decayed', the cat would ultimately

[2]If someone has forgotten whether or not they have food in their fridge, their fridge is not in a macroscopic superposition of 'empty' and 'full'. Instead, they are a simply a forgetful person.

evolve to be in a macroscopic superposition of 'alive' and 'dead'.

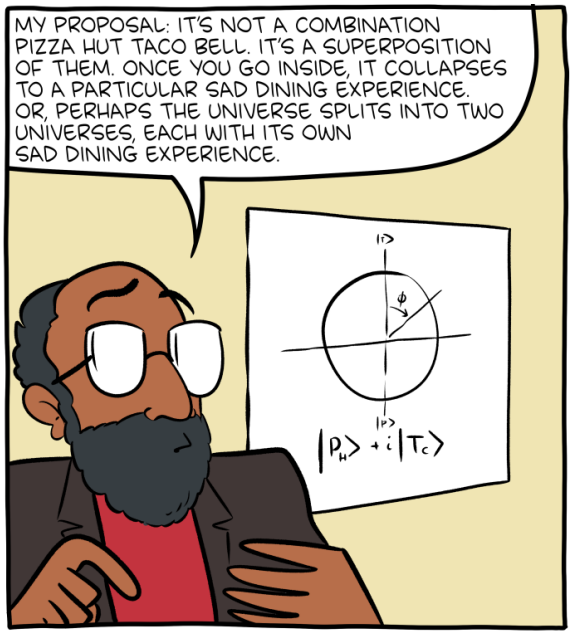


Figure 2.2: It is worth stressing that quantum properties such as *superposition* and *entanglement* are theoretically possible at a macroscopic level, but are not observed [Zur06]. Ergo, quantum effects are difficult to visualize. Illustration by Zach Weinersmith, *Saturday Morning Breakfast Cereal: Quantum-2* (2019), see [Wei19] in the bibliography for the source details.

In general, a quantum state $|\psi\rangle$ in the composite Hilbert space $\bigotimes_{k=1}^{n} \mathcal{H}_{A_k}$ is called separable if and only if there exists $|\psi_{A_k}\rangle \in \mathcal{H}_{A_k}$ for all k such that

$$|\psi\rangle = \bigotimes_{k=1}^{n} |\psi_{A_k}\rangle\,, \tag{2.6}$$

otherwise it is entangled. For example, the n qubit Greenberger–Horne–Zeilinger (GHZ) state

$$|\psi_{\text{GHZ}}\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\,\big), \tag{2.7}$$

is a highly entangled state with many practical applications, including quantum metrology. GHZ states are the canonical resource for the quantum metrology problem of phase estimation [GLM04; TA14]. The utility of a GHZ state is frequently referenced in this thesis and used as a benchmark in **Chapter 4** and **Chapter 5**.

Although quantum entanglement was originally coined as *spooky* by Einstein

[EPR35], it has since been shown to be a valuable resource for the field of quantum information. Numerous quantum-based protocols (e.g. superdense coding [BW92], teleportation [Ben+93]) are contingent on the non-classical correlations of entangled quantum states. Quantum metrology is no different: entanglement[3] allows for estimation strategies to surpass the limits of classical statistics [GLM04; GLM06; GLM11; TA14].

2.1.3 Mixed States

It is often practical to consider statistical ensembles of quantum states $\{(p_i, |\psi_i\rangle)\}$, where p_i is the probability of the system being in the quantum state $|\psi_i\rangle$. This abstraction is useful to incorporate stochastic processes and classical randomness into the description of a quantum system. Mathematically this is represented as a linear and positive semi-definite[4] operator

$$\rho = \sum_i p_i \, |\psi_i\rangle\langle\psi_i| \,, \tag{2.8}$$

which is often referred to as a density operator, density matrix or (most commonly) a *mixed state*. Because the set $\{p_i\}$ represents a set of classical probabilities, we must have that $\sum_i p_i = 1$, from which it follows that all mixed states have unit trace $\mathrm{Tr}\,\rho = 1$. The purity of a mixed state is a measure on the classical randomness present in a quantum system and defined by $\mathrm{Tr}\,\rho^2$. For a general mixed state $0 \leq \mathrm{Tr}\,\rho^2 \leq 1$, and the upper-bound is saturated if and only if there is no inherent classical randomness present, i.e. the system is in a definite quantum state - more commonly referred to as a *pure state*. Density operator formalism is predominantly used in this thesis and, depending on the context, may signify a general mixed state or specifically a pure state.

When dealing with composite systems, $\rho_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, it can be beneficial to describe a subsystem when one does not have access to the other systems, e.g. A does not have access to B. This is better known as a reduced density operator and can be computed via the partial-trace

$$\rho_A = \mathrm{Tr}_B\, \rho_{AB} = \sum_k \langle b_k|\rho_{AB}|b_k\rangle \,, \tag{2.9}$$

[3] In continuous variable systems, non-classical correlations can also be achieved through a process called squeezing [Lvo15]. Squeezing is not the same as entanglement, but also leads to a quantum advantage for metrology problems [Cav81; DJK15; Sch17].

[4] ρ is positive semi-definite if $\langle\phi|\rho|\phi\rangle \geq 0 \; \forall \, |\phi\rangle \in \mathcal{H}$.

where $\{|b_k\rangle\}$ is any orthonormal basis of $\mathcal{H}_B$. If a composite system is an entangled pure quantum state, then the reduced density operator is guaranteed to be a mixed state with purity less than one. Therefore, by discarding a portion of a composite quantum system, one introduces classical randomness into the non-discarded systems.

The opposite is similarly true, in that it can be beneficial to extend the Hilbert space of a mixed state to a composite system in which it is a pure state. This is known as a purification process. If $\rho_A = \sum_i p_i |\psi_i\rangle\langle\psi_i| \in \mathcal{H}_A$ and $\mathcal{H}_B$ is an auxiliary Hilbert space with orthonormal basis $\{|\phi_i\rangle\}$, then the pure state

$$|\Psi_{AB}\rangle = \sum_i \sqrt{p_i} |\psi_i\rangle |\phi_i\rangle \tag{2.10}$$

is a purification of ρ_A because $\mathrm{Tr}_B |\Psi_{AB}\rangle\langle\Psi_{AB}| = \rho_A$. The purification is not unique.

2.1.4 Vector And Matrix Representation

Up until now, pure states have been represented as an abstract mathematical element of a Hilbert space, and general mixed states as a linear and non-negative operator acting on said Hilbert space. For the most part of this thesis, this abstract representation is sufficient. However, some of the mathematical derivations in **Appendix B** make use of an alternative representation using vectors and matrices.

The vector representation of a pure qubit state is a two dimensional[5] column vector

$$\alpha |0\rangle + \beta |1\rangle \longleftrightarrow \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \tag{2.11}$$

and the representation of the corresponding dual is a two-dimensional row vector

$$\alpha^* \langle 0| + \beta^* \langle 1| \longleftrightarrow \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}. \tag{2.12}$$

Combining the above, the mixed state $\{(p_1, \alpha |0\rangle + \beta |1\rangle), (p_2, \gamma |0\rangle + \delta |1\rangle)\}$ is represented with the matrix

$$p_1 \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} + p_2 \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \begin{pmatrix} \gamma^* & \delta^* \end{pmatrix} = \begin{pmatrix} p_1|\alpha|^2 + p_2|\gamma|^2 & p_1\alpha\beta^* + p_2\gamma\delta^* \\ p_1\alpha^*\beta + p_2\gamma^*\delta & p_1|\beta|^2 + p_2|\delta|^2 \end{pmatrix}. \tag{2.13}$$

[5] This representation extends to qudits, where the vectors are d dimensional objects.

2.2 Quantum Operations

Operator formalism in quantum mechanics is used to describe transformations to quantum states[6]. At the most general level, a *quantum operator* Γ is a linear map from an input Hilbert space $\mathcal{H}_1$ to an output Hilbert space $\mathcal{H}_2$

$$\begin{aligned} \Gamma : \mathcal{H}_1 &\to \mathcal{H}_2 \\ \rho &\to \Gamma(\rho). \end{aligned} \tag{2.14}$$

It is demanded that Γ has two properties. The first is for $\Gamma(\rho)$ to have unit-trace (for it to qualify as a quantum state); this is known as being *trace-preserving*. The second is for $\Gamma(\rho)$ to be positive semi-definite, and more so, if a partial trace is taken, then the remaining subsystem is also positive semi-definite; this is known as being *completely positive*. If Γ satisfies both properties, it is called a completely positive trace-preserving (CPTP) map. A CPTP map can be written in the form

$$\Gamma(\rho) = \sum_j A_j \rho A_j^\dagger, \tag{2.15}$$

where $\{A_j\}$ are known as Kraus operators [HK69] which satisfy $\sum_j A_j A_j^\dagger = \mathbb{I}$.

2.2.1 Pauli And Clifford Operators

The three Pauli operators, X, Y and Z, are conceivably the most widely used operators in the field quantum information. The Pauli operators are Hermitian and involutory operators which act on single qubit quantum states, and along with the identity map, form a group. Listed are the bra-ket and matrix representations of

[6] In this thesis, quantum states are viewed as the *variables*, this is known as the Schrödinger picture. There is another formulation in which the operators act as the *variables*, better known as the Heisenberg picture [GS18].

the Pauli operators:

$$X = |0\rangle\langle 1| + |1\rangle\langle 0| \to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.16}$$

$$Y = -i\,|0\rangle\langle 1| + i\,|1\rangle\langle 0| \to \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{2.17}$$

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| \to \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.18}$$

The Pauli group $\{\mathbb{I}, X, Y, Z\}$ is a basis for all 2×2 complex matrices, and thus a single qubit quantum state can be expressed as

$$\rho = \frac{1}{2}\Big(\mathbb{I} + \mathrm{Tr}(X\rho)X + \mathrm{Tr}(Y\rho)Y + \mathrm{Tr}(Z\rho)Z\Big). \tag{2.19}$$

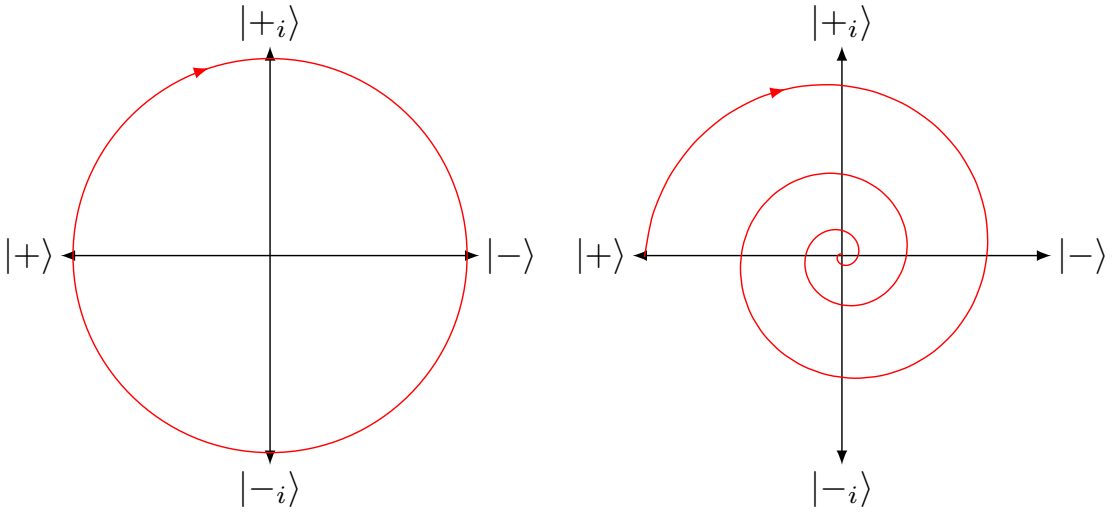
In general, defining the mth degree Pauli group to be $\mathcal{P}_m = \{\mathbb{I}, X, Y, Z\}^{\otimes m}$, a quantum system composed of m qubits can be expressed as

$$\rho = \frac{1}{2^m} \sum_{P \in \mathcal{P}_m} \mathrm{Tr}(P\rho)P. \tag{2.20}$$

Another class of operators which are well known is the Clifford group. The Clifford group is an important set of unitary operators in the realm of quantum computing and quantum algorithms, as they were shown to be efficiently simulated with a classical computer [Got98]. Mathematically, the Clifford group of degree m, denoted $\mathcal{C}_m$, is the set of unitary operators which normalize $\mathcal{P}_m$ (up to a phase of ± 1), thus $\forall C \in \mathcal{C}_m$ and $\forall P \in \mathcal{P}_m$

$$CPC^\dagger \in \pm\mathcal{P}_m. \tag{2.21}$$

The set of local Clifford operations $\mathcal{C}_1$ can be decomposed as a sequence of a Pauli operations or a $\pi/4$ phase shift $e^{\pm i\frac{\pi}{4}P}$ (with $P \in \{X, Y, Z\}$). Evidently, C_1 is much simpler to implement than an arbitrary local unitary [NWD14]. For this reason, all but one of the cryptographic protocols we devise in **Chapter 6** consist solely of local Clifford operations.



(a) Unitary evolution. (b) Environmental decoherence.

Figure 2.3: Visual representation of the dynamics of a single qubit (initialized in the $|+\rangle$ state) is governed by the master equation $\frac{d\rho(t)}{dt} = -\frac{i}{\hbar}[\frac{\omega}{2}Z, \rho(t)] + \gamma\big((X\rho(t)X - \rho(t)\big)$. The evolution of the qubit traces a path in the $X-Y$ plane of the Bloch sphere. In (a) the environmental term is ignored ($\gamma = 0$) and the qubit forever oscillates between $|+\rangle$ and $|-\rangle$ with frequency ω. In (b) the decoherence term ($\gamma \neq 0$) causes the qubit to eventually decohere to the maximally mixed state (the center of the Bloch sphere).

2.2.2 Dynamics

The parameter encoding mechanism is the predominant element in a quantum metrology problem. Formally, this is a physical process which influences the evolution of a quantum state. In a closed and isolated system with a Hamiltonian H, the evolution of a quantum state ρ is governed by the Schrödinger equation [Sch26; GS18]

$$\frac{d\rho(t)}{dt} = -\frac{i}{\hbar}[H, \rho(t)]. \tag{2.22}$$

As a result, the evolution is described as a unitary transformation

$$\rho(t) = U_{t-t_0}\rho(t_0)U_{t-t_0}^{\dagger}, \tag{2.23}$$

where $U_\tau = e^{-\frac{i}{\hbar}H\tau}$.

It is worth noting that closed and isolated systems do not emulate reality and are effectively a fantasy for experimentalists and engineers. Real world quantum technologies are plagued with noise (the subject of **Chapter 5**) due to interac-

tions with the environment [Gar91; BP+02]. As a result, information is lost to the surroundings, causing decoherence, dephasing, losses and fluctuations. There is no explicit equation which governs the evolution of a quantum system for a general environmental interaction. However, with some assumptions (namely that the system and environment are weakly-coupled and the interaction is time-independent) then one can model evolution by modifying the Schrödinger equation [BP+02]

$$\dot{\rho}(t) = -\frac{i}{\hbar}[H, \rho(t)] + \mathcal{L}\big(\rho(t)\big), \tag{2.24}$$

where the super-operator $\mathcal{L}$ is better known as the Liouvillian. It was demonstrated that for the evolution to yield a valid transformation (CPTP), the Liouvillian will take on the form [Lin76]

$$\mathcal{L}\big(\rho(t)\big) = \sum_{j=1}^{d^2-1} \gamma_j \big[L_k \rho(t) L_k^\dagger - \frac{1}{2}\{\rho(t), L_k L_k^\dagger\}\big], \tag{2.25}$$

where d is the dimension of the Hilbert space, γ_j are non-negative decay rates, and $L_1, \ldots, L_{d^2-1}$ are Lindblad operators. This equation is often referred to as the Lindblad master equation.

The contrast between the Schrödinger equation and the Linblad master equation is depicted in Fig. (2.3). When a single qubit pure state is governed solely by unitary dynamics, it perpetually oscillates between pure states. But, when the system is coupled to the environment, the qubit spirals towards the maximally mixed state.

2.3 Quantum Measurements

The principal goal of quantum metrology is to use a quantum system to estimate the value a physical unknown parameter. With this in mind, it is crucial to extract physical information from a quantum system; in the language of quantum mechanics, this is done by measuring an *observable* [Von18]. Formally, a (finite) observable O is a linear and Hermitian ($O = O^\dagger$) operator. By the spectral value theorem, O can be decomposed into a set of projectors $\{P_i\}$ satisfying $P_i P_j = P_i \delta_{i,j}$ and $\sum_i P_i = \mathbb{I}$ along with a corresponding set of real-values eigenvalues $\{o_i\}$ such that $O = \sum_i o_i P_i$. Here, the index i signifies different measurement outcomes. If the quantum state ρ is measured, then outcome i is observed with probability $\mathrm{Tr}(P_i\rho)$ and the expectation value of O is $\langle O \rangle = \sum_i o_i \,\mathrm{Tr}(P_i\rho) = \mathrm{Tr}(O\rho)$. This is the simplest description of a

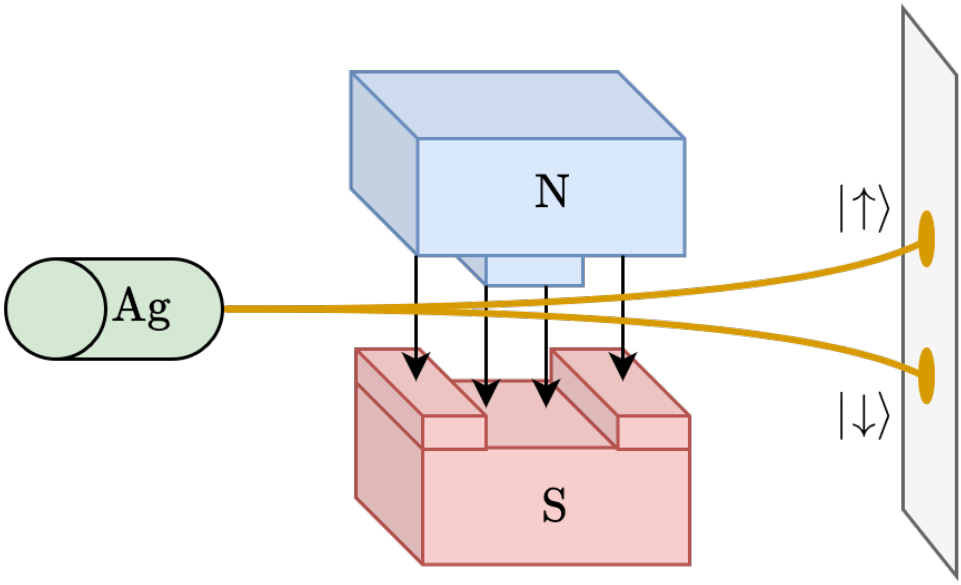


Figure 2.4: The Stern-Gerlach experiment [GS22] is an early prototype for a quantum measurement. A beam of silver (Ag) atoms is sent through an inhomogeneous magnetic field towards a detector screen. Initially, the spin of the silver atoms are in arbitrary superpositions of $|\uparrow\rangle$ and $|\downarrow\rangle$. Classical physics predicts that the silver atoms would be detected along the length of the detector screen. Instead, the silver atoms were detected in two bunches, one bunch of spin $|\uparrow\rangle$ atoms and one bunch of spin $|\downarrow\rangle$ atoms.

quantum measurement, and is called a projection-valued measurement (PVM).

A quantum measurement can be further generalized by abandoning the notion that measurement outcomes are orthogonal. This abstraction is called a positive-operator-valued measure (POVM) [NC02; Jac14]. A POVM is designed to accompany any allowable measurement statistics, bearing in mind that the post-measurement state is ambiguous (see the next subsection). A POVM can be described by a set of positive semi-definite operators $\{M_m\}$ which satisfy the completeness relationship $\sum_m M_m = \mathbb{I}$. The outcome m is observed with probability $\mathrm{Tr}(M_m\rho)$. Comparable to the purification of mixed states, Eq. (2.10), it has been shown that a POVM can always be obtained from a PVM acting on a higher dimensional space [NC02].

In this thesis we focus on single parameter quantum metrology problems. Although many of the results naturally generalize to multiparameter problems, it is important to be cognisant of the incompatibility of simultaneous measurements in the multiparameter setting. Specifically, if two observables, A and B, do not com-

mute

$$[A, B] \neq 0, \tag{2.26}$$

then measuring A and then B is different than measuring B then A. In fact, this is one of the major reasons why the cryptographic protocols outlined in **Chapter 6** can be deemed secure. The incompatibility of simultaneous measurements gives rise to the famous Heisenberg uncertainty principle [Rob29]

$$\Delta^2 A \Delta^2 B \geq \frac{1}{4} \left| \langle [A, B] \rangle \right|^2, \tag{2.27}$$

where $\Delta^2 A = \langle A^2 \rangle - \langle A \rangle^2$ is the variance of an observable.

2.3.1 Collapse Of The Wave Function

After a measurement is performed the quantum state undergoes a non-unitary transformation, more commonly referred to as the 'collapse of the wave function'[7]. If a PVM is performed on the state ρ and outcome i is observed, then

$$\rho \to \frac{P_i \rho P_i}{\mathrm{Tr}(P_i \rho)}. \tag{2.28}$$

The post-measurement state is drastically more complex when considering a general POVM. As mentioned, the post-measurement state is ambiguous, this is in consequence to the POVM elements $\{M_m\}$ not having a unique Kraus decomposition [HK69], as a multitude of measurement schemes may result in the same measurement statistics [Jac14]. A Kraus decomposition of M_m is a product of an (not necessarily self-adjoint) operator with its conjugate transpose, i.e for each M_m there exists an A_m such that $M_m = A_m A_m^\dagger$. The set $\{A_m\}$ are the measurement operators which define a physical process which corresponds with the POVM. For a specific set of measurement operators, if outcome m is observed, then

$$\rho \to \frac{A_m \rho A_m^\dagger}{\mathrm{Tr}(M_m \rho)}. \tag{2.29}$$

By comparing Eq. (2.28) and Eq. (2.29), one can interpret a PVM as a special case of a POVM when the set of measurement operators are all projectors.

[7] The collapse of the wave function, a postulate of the Copenhagen interpretation, is arguably the most widely used model for quantum measurements. It is important to note though, to date, the dynamics of quantum measurements are still debated [Zeh70; Sch05].

2.4 Distance Measures

Quantum states are elements of a Hilbert space, so it is natural to consider the proximity of quantum states. Distance measures can be useful, as quantum states which are *close* to one another can be expected to behave similarly under appropriate transformations. Distance measures, namely the trace-distance and fidelity, play a crucial role in **Chapter 6**, where the quantum states in question are bounded with respect to the above measures, from which, their utility for quantum metrology can be gauged.

2.4.1 Trace Distance

The trace distance, denoted by $\mathscr{D}$, between quantum states ρ and σ can be calculated using

$$\mathscr{D}\big(\rho,\sigma\big) = \frac{1}{2}\operatorname{Tr}|\rho-\sigma|, \tag{2.30}$$

where $|A| = \sqrt{A^\dagger A}$. An alternative definition of the trace distance can be expressed in terms of POVMs. Let $\{M_m\}$ be a POVM, in which outcome m is witnessed with probabilities $p_m = \operatorname{Tr}(M_m\rho)$ and $q_m = \operatorname{Tr}(M_m\sigma)$. The trace distance is equivalently defined via

$$\mathscr{D}\big(\rho,\sigma\big) = \max_{\{M_m\}}\Big(\frac{1}{2}\sum_m |p_m - q_m|\Big), \tag{2.31}$$

where the maximization is taken over all POVMs. The contents of the brackets on the right-hand side of the above equation is in fact the definition of the trace distance between probability distributions $\{p_m\}$ and $\{q_m\}$ [NC02]. The second expression listed to compute the trace distance between quantum states is certainly impractical to calculate, however it does provide an insightful inequality: for any POVM $\{M_m\}$, it follows that

$$\frac{1}{2}\sum_m |\operatorname{Tr}\big(M_m(\rho-\sigma)\big)| \leq \mathscr{D}\big(\rho,\sigma\big). \tag{2.32}$$

The trace distance is contractive under a CPTP map $\mathcal{E}$, that is

$$\mathscr{D}\big(\mathcal{E}(\rho),\mathcal{E}(\sigma)\big) \leq \mathscr{D}\big(\rho,\sigma\big). \tag{2.33}$$

2.4.2 Fidelity

The fidelity between quantum states is perhaps the most renowned measure of closeness in quantum information, even though it is not a metric in the mathematical sense. The fidelity, denoted with $\mathscr{F}$, between quantum states ρ and σ can be computed using

$$\mathscr{F}\big(\rho,\sigma\big) = \Big(\operatorname{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\Big)^2, \tag{2.34}$$

which greatly simplifies to $\mathscr{F}\big(\rho,\sigma\big) = \operatorname{Tr}(\rho\sigma)$ when either ρ or σ is a pure state. Note that this version of the fidelity is the square of what is defined in [NC02]. The fidelity and trace distance are related by the Fuchs–van de Graaf inequalities [FV99]

$$1 - \sqrt{\mathscr{F}\big(\rho,\sigma\big)} \leq \mathscr{D}\big(\rho,\sigma\big) \leq \sqrt{1 - \mathscr{F}\big(\rho,\sigma\big)}. \tag{2.35}$$

3
Estimation Theory

Estimation theory is the mathematical language of metrology. Statistical error in classical estimation theory is ultimately constrained by the central limit theorem. *Quantum metrology* overcomes this limitation thanks to quantum entanglement. With the vast number of applications and straightforward proof of principle, it is unsurprising that quantum metrology is witnessing a boon of theoretical and experimental developments [GLM11; DRC17; Pir+18].

This chapter is divided into three sections. The first section summarizes important concepts from classical estimation theory [Kay93; Cox06; She03; Ric06; Poo13]. The second section is devoted to the analogous concepts of quantum estimation theory formalized by Helstrom [Hel67; Hel68; Hel69] and Holevo [Hol73; Hol82]. The final section examines example applications of quantum metrology (phase estimation and amplitude estimation) to put into perspective the mathematical tools and concepts introduced throughout the first two sections. For a quantum information perspective on quantum metrology see [TA14]. For a more mathematical rigorous review of quantum metrology and quantum estimation theory see [SJS17]. For more information on estimation theory and statistical inference see [Kay93; Cox06].

> *An experiment is a question which science poses to Nature and a measurement is the recording of Nature's answer.*
>
> -Max Planck

3.1 Classical Estimation Theory

In an abstract sense, the scientific and mathematical knowledge of humankind is reflected in the mathematical models used to describe the contents of the universe:

planetary orbits, bacterial growth in a petri dish, even social constructs like financial trends. These models, are not fabricated haphazardly, instead they are a manifestation of a multitude of observations and tested by making predictions. As our efficiency of gathering and interpreting data increases, so do the mathematical models, and in turn our understanding of the universe. For example, the theory of gravity has evolved along with the capabilities of telescopes; from Galilean and Newtonian gravity to Einstein's theory of general relativity to the (currently unconfirmed) theory of dark matter and dark energy.

Estimation theory is a branch of statistics at the heart of mathematical modelling. It addresses the question: 'What is the most efficient way of extracting information from a set of data?'. This seemingly simple question is difficult to answer. Typically, the variables used to describe a mathematical model can be partitioned in two categories

1. observables - an attribute which can be inherently measured (e.g. position and speed).

2. latent parameters - an attribute which cannot be inherently measured, (e.g. strength of an electromagnetic field).

The *parameter estimation problem* is concerned with the extent at which collected data (observables) can be used to estimate the unknown latent parameters [She03]. With respect to the listed examples, one could observe the dynamics of a charged particle to estimate the strength of an electromagnetic field.

Formally, observed data $\mathbf{x} = \{x_1, \ldots, x_N\}$ is treated as a realisation of N independent and identically distributed (iid) random variables X. A probably density function $p(X|\theta)$ dictates the distribution of observed data, where θ is a latent parameter. The goal of the parameter estimation problem is to construct an *estimator* $\hat{\theta}(\mathbf{x})$, which should be interpreted as a function whose input is the collected data $\mathbf{x}$ and outputs an estimate of θ. The explicit dependence on $\mathbf{x}$ is sometimes dropped for clarity, $\hat{\theta}(\mathbf{x}) \to \hat{\theta}$. Estimators are subjected to two conditions. The first condition is that the expected estimate is the true value of the parameter, this is known as having an unbiased estimator

$$\langle \hat{\theta} \rangle = \int p(\mathbf{x}|\theta)\hat{\theta}(\mathbf{x})\mathrm{d}\mathbf{x} = \theta. \tag{3.1}$$

The integral equation is used for observed data which can take on a continuum of values, it is interchangeable with a sum in the discrete case. The second condition is

that an estimator tends towards the correct value as the amount of data increases, this is known as being consistent

$$\lim_{N\to\infty} \hat{\theta} = \theta. \tag{3.2}$$

An estimator is a manifestation of random variables, and is thus also a random variable, hence, statistical moments such as mean and variance are well-defined.

The statistical inference process adopted to the parameter estimation problem is dependent on the nature of the latent variable: deterministic or stochastic. Usually, a frequentist inference approach is taken for deterministic parameters and a Bayesian inference approach is taken for stochastic parameters [Li+18]. Mathematically, these two approaches vary greatly, the primary differences are listed in Tab. (3.1), but they are not mutually exclusive. The subsequent chapters of this thesis employ the frequentist approach, and therefore the frequentist approach is summarized in greater detail in this chapter. That being said, the Bayesian approach has been adapted to the realm of quantum information [Hol82; TWC11], and has been gaining traction in the community [Ber+09; GM13; JD15; WG16; RD20]. Specifically, to circumvent problems of the frequentist approach: i) lack of a priori knowledge [KD10; Dem11] and ii) inaccuracies with limited resources [RD20]. Even though it is not applied to the research presented in this thesis, for the sake of completeness, a brief summary of the Bayesian approach used in classical parameter estimation problems and its adaptation to quantum parameter estimation problems is included in this chapter.

	Frequentist Approach	Bayesian Approach
Parameter(s)	Deterministic	Stochastic
Figure of Merit	Mean squared error	Cost function
Optimization	Local	Global

Table 3.1: The main differences between the frequentist approach and Bayesian approach for statistical inference. This is a broad perspective and the statistical inference approaches are not restricted by this table.

3.1.1 The Frequentist Approach

The *frequentist approach* is typically used when θ is deterministic (sometimes called static). As $N \to \infty$ the frequency of collected data tends to reflect the probability density function, hence the etymology. Therefore with a sufficient amount of collected data, the unknown parameter can be estimated to any desired precision. The figure of merit used by the frequentist approach is the mean-squared error (MSE)

$$\Delta^2\hat{\theta} = \langle(\hat{\theta} - \theta)^2\rangle = \int p(\mathbf{x}|\theta)\big(\hat{\theta}(\mathbf{x}) - \theta\big)^2 \mathrm{d}\mathbf{x}, \tag{3.3}$$

in which the aim is to find an estimator which minimizes the above equation. Because the estimator is assumed to be unbiased, the MSE is equal to the variance, which is often a more significant statistical quantity.

The first controversy of the the frequentist approach arises due to the fact that an optimal estimator (one where Eq. (3.3) is minimized) is potentially dependent on θ. Some estimators may be optimal for specific values of θ (local), whereas an estimator which is optimal for all values of θ (global) can only be worse than ones which are locally optimized. At first glance, this appears counter intuitive because a locally optimized estimator requires exact knowledge of θ, which defeats the purpose of parameter estimation. However, it is reasonable to assume that a priori approximate knowledge $\theta \approx \theta_0$ is often known because of theory or previous estimates. In the absence of a priori knowledge, one can construct a locally efficient estimator by increasing N. To do so, a fraction of the results are first used to obtain a local approximation θ_0, and the remaining are used within the locally optimized estimator. Unfortunately, the frequentist approach does not provide a method on bounding N such that the local regime can be assured; thus the saturation of an optimal estimator may not be possible without the ability to infinitely increase N.

3.1.2 Cramér-Rao Bound And Fisher Information

The *Cramér-Rao Bound* (CRB) is an inequality which assigns a lower bound to the MSE of unbiased estimators [Cra46], the derivation of which is straightforward. The unbiased condition, Eq. (3.1), can be re-written as

$$\int p(\mathbf{x}|\theta)\big(\hat{\theta}(\mathbf{x}) - \theta\big)\mathrm{d}\mathbf{x} = 0, \tag{3.4}$$

from which it follows that

$$\begin{aligned} 0 &= \frac{\partial}{\partial\theta}\int p(\mathbf{x}|\theta)\big(\hat{\theta}(\mathbf{x})-\theta\big)\mathrm{d}\mathbf{x} \\ &= \int \frac{\partial p(\mathbf{x}|\theta)}{\partial\theta}\big(\hat{\theta}(\mathbf{x})-\theta\big)\mathrm{d}\mathbf{x} - \int p(\mathbf{x}|\theta)\mathrm{d}\mathbf{x} \\ &= \int p(\mathbf{x}|\theta)\frac{\partial \ln p(\mathbf{x}|\theta)}{\partial\theta}\big(\hat{\theta}(\mathbf{x})-\theta\big)\mathrm{d}\mathbf{x} - 1. \end{aligned} \tag{3.5}$$

Using the Cauchy–Schwarz inequality

$$\left|\int f(x)g(x)\mathrm{d}x\right|^2 \leq \left(\int f(x)^2\mathrm{d}x\right)\cdot\left(\int g(x)^2\mathrm{d}x\right), \tag{3.6}$$

with $x \to \mathbf{x}$, $f(x) \to \sqrt{p(\mathbf{x}|\theta)}\frac{\partial \ln p(\mathbf{x}|\theta)}{\partial\theta}$ and $g(x) \to \sqrt{p(\mathbf{x}|\theta)}\big(\hat{\theta}(\mathbf{x})-\theta\big)$, Eq. (3.5) is transformed into the inequality

$$1 \leq \left(\int p(\mathbf{x}|\theta)\big(\hat{\theta}(\mathbf{x})-\theta\big)^2\mathrm{d}\mathbf{x}\right)\cdot\left(\int p(\mathbf{x}|\theta)\Big(\frac{\partial \ln p(\mathbf{x}|\theta)}{\partial\theta}\Big)^2\mathrm{d}\mathbf{x}\right). \tag{3.7}$$

The above can be manipulated to obtain the CRB

$$\Delta^2\hat{\theta} \geq \frac{1}{\mathcal{I}\big(p(\mathbf{x}|\theta)\big)}, \tag{3.8}$$

where

$$\begin{aligned} \mathcal{I}\big(p(\mathbf{x}|\theta)\big) &= \int p(\mathbf{x}|\theta)\Big(\frac{\partial \ln p(\mathbf{x}|\theta)}{\partial\theta}\Big)^2\mathrm{d}\mathbf{x} \\ &= \int \frac{1}{p(\mathbf{x}|\theta)}\Big(\frac{\partial p(\mathbf{x}|\theta)}{\partial\theta}\Big)^2\mathrm{d}\mathbf{x} \\ &= -\int p(\mathbf{x}|\theta)\frac{\partial^2 \ln p(\mathbf{x}|\theta)}{\partial\theta^2}\mathrm{d}\mathbf{x} \end{aligned} \tag{3.9}$$

is the *Fisher Information* (FI), where three equivalent (assuming that p is twice differentiable) expressions given. The FI is a non-negative and additive quantity. Because $\mathbf{x}$ is N independent realisations of the random variable X, the CRB can be equivalently expressed as

$$\Delta^2\hat{\theta} \geq \frac{1}{N\mathcal{I}\big(p(X|\theta)\big)}. \tag{3.10}$$

The above form of the CRB reflects the limitations of central limit theorem: as $N \to \infty$ the sample average will take on a normal distribution with a variance of

$\mathcal{O}\big(N^{-1}\big)$.

The FI is often interpreted as a measure of how much information about an unknown parameter can be extracted from a probability density function [Fis25]. In particular, θ can be learned perfectly when $\mathcal{I} \to \infty$, and conversely no information can be learned about θ when $\mathcal{I} = 0$. In fact, when viewing probability density functions as points on a manifold (parameterized by θ), the FI is a Riemannian metric between neighbouring probability density functions $p(X|\theta)$ and $p(X|\theta + \delta\theta)$ [Nie13]. Similarly, the statistical angle[1] between probability density functions

$$D\big(p_1(x), p_2(x)\big) = \arccos \int \sqrt{p_1(x)p_2(x)}\mathrm{d}x, \tag{3.11}$$

can be expressed as [BCR86]

$$D\big(p(X|\theta), p(X|\theta+\delta\theta)\big) = \frac{1}{2}\sqrt{\mathcal{I}\big(p(X|\theta)\big)}\delta\theta + \mathcal{O}\big(\delta\theta^2\big). \tag{3.12}$$

Hence, a probability density function with a high FI will deviate more upon small perturbations $\delta\theta$ than the opposing case of a probability density function with a small FI.

The Cauchy-Schwarz inequality, Eq. (3.6), is saturated if

$$\frac{|f(x)|}{|g(x)|} = \frac{\int f(x)^2\mathrm{d}x}{\int g(x)^2\mathrm{d}x} \tag{3.13}$$

Therefore an estimator which saturates the CRB for all θ (global) satisfies

$$\frac{\partial \ln p(\mathbf{x}|\theta)}{\partial\theta} = \mathcal{I}\big(\mathbf{x}|\theta\big)\big(\hat{\theta}(\mathbf{x}) - \theta\big). \tag{3.14}$$

An estimator which saturated the CRB is said to be *efficient*. The above expression can be equivalently written as

$$\begin{aligned} p(\mathbf{x}|\theta) &= \exp\left(\int \mathcal{I}\big(\mathbf{x}|\theta\big)\big(\hat{\theta}(\mathbf{x}) - \theta\big)\mathrm{d}\theta\right) \\ &= \exp\left(\frac{\partial\mathcal{J}\big(\mathbf{x}|\theta\big)}{\partial\theta}\big(\hat{\theta}(\mathbf{x}) - \theta\big) + \mathcal{J}\big(\mathbf{x}|\theta\big) + c(\mathbf{x})\right), \end{aligned} \tag{3.15}$$

where $\mathcal{J}\big(\mathbf{x}|\theta\big)$ is a function which satisfies $\frac{\partial^2\mathcal{J}\left(\mathbf{x}|\theta\right)}{\partial\theta^2} = \mathcal{I}\big(\mathbf{x}|\theta\big)$ and $c(\mathbf{x})$ is an arbitrary function independent of θ, both of which are chosen such that the unbiased condition,

[1] This is the classical version of the Bures angle [Woo81].

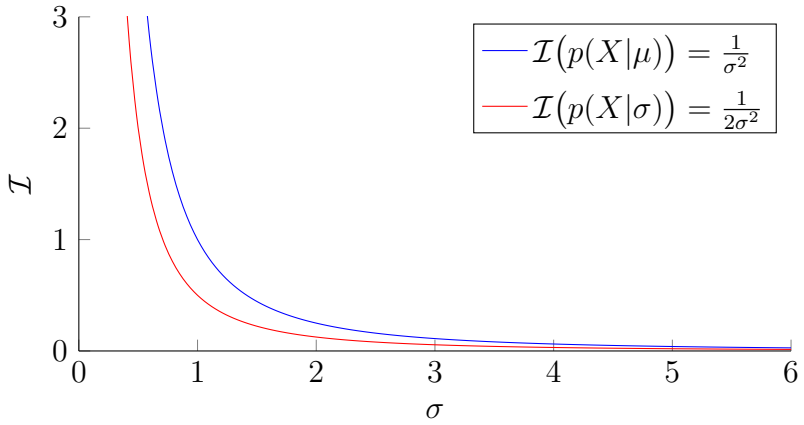
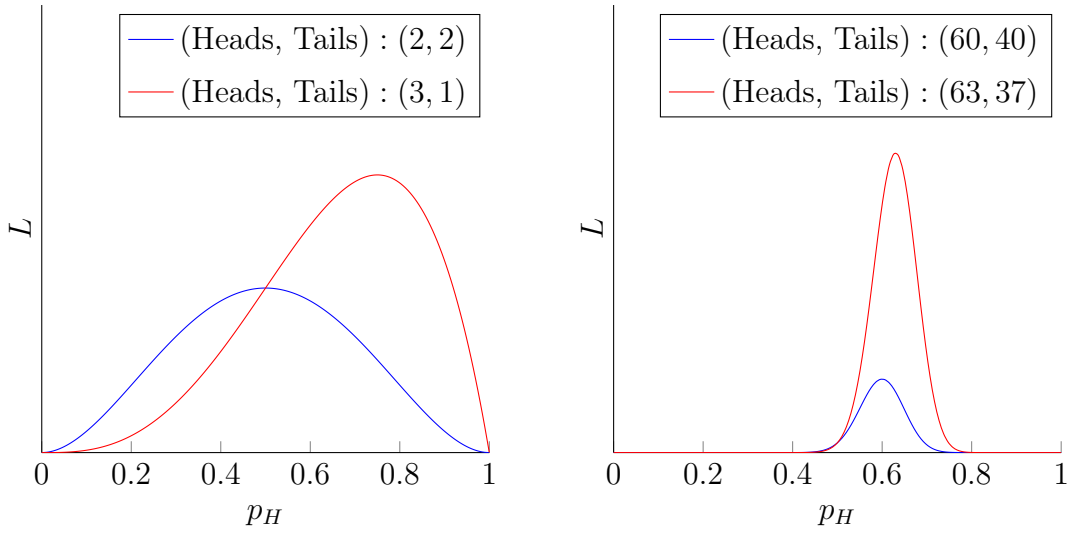


Figure 3.1: The FI for a normal distribution $p(X|\mu,\sigma) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{1}{2}(\frac{x-\mu}{\sigma})^2}$. Regardless of whether μ or σ is the latent parameter, the FI is exclusively dependent on the standard deviation of the normal distribution. This is logical because it is more difficult to interpret data with a larger standard deviation; which is in accordance with the interpretation of the FI being a measure of extractable information. One could equally consider the scenario in which both μ and σ are unknown parameters. Here multiparameter parameter estimation techniques are needed - which are discussed in a latter part of this chapter.

Eq. (3.1), is satisfied. This general expression for a probability density function can correspond to a multitude of well-known distributions in statistics with exponential tendencies: Gaussian, Bernoulli, Poisson, et cetera. It should be stressed that an efficient global estimator does not necessarily exist, further it may encounter the earlier stated problem of having a dependence on θ. A locally (approximately) efficient estimator can be constructed with prior knowledge that $\theta \approx \theta_0$ by re-arranging Eq. (3.14)

$$\hat{\theta}_{\text{Local}} = \theta_0 + \frac{1}{\mathcal{I}\big(\mathbf{x}|\theta_0\big)} \frac{\partial \ln p(\mathbf{x}|\theta)}{\partial \theta}\bigg|_{\theta\to\theta_0}. \tag{3.16}$$

Unfortunately, the locally approximate estimator is ultimately constrained by ones prior knowledge, as shifting $\theta_0 \to \theta_0 + \delta\theta_0$ will similarly shift Eq. (3.16) by $\mathcal{O}(\delta\theta_0)$. Furthermore, the locally approximate estimator may be ill defined on certain domains, for example one of circular symmetry (such as the problem of phase estimation which is discussed in a later section of this chapter).



(a) $N = 4$ (b) $N = 100$

Figure 3.2: Likelihood function for a biased coin where p_H is an unknown probability of the coin toss resulting in heads. The maximum likelihood estimation strategy outputs $\hat{p}_H = \frac{\#\text{ Heads}}{N}$. The estimate is sensitive to small fluctuations in the observed data for small N (a), but becomes more robust to fluctuations as N increases (b).

3.1.3 Maximum Likelihood Estimation

The *likelihood function* $L(\theta|\mathbf{x}) = p(\mathbf{x}|\theta)$ is a goodness of fit between a model and the sampled data. It should be understood that the likelihood function is not a probability density function; the observed data $\mathbf{x}$ is held fixed and the latent parameter θ is considered a variable. The intuition is simplistic: if $L(\theta_1|\mathbf{x}) > L(\theta_2|\mathbf{x})$, then it is more likely that the true value of θ is θ_1 rather than θ_2. This is the principal idea of maximum likelihood estimation [BW88]. The maximum likelihood estimator, $\hat{\theta}_{\text{ML}}$, outputs the value of θ which maximizes $L(\theta|\mathbf{x})$

$$\hat{\theta}_{\text{ML}}(\mathbf{x}) = \underset{\theta}{\text{argmax}} L(\theta|\mathbf{x}) = \underset{\theta}{\text{argmax}} \ln L(\theta|\mathbf{x}). \tag{3.17}$$

Because $p(\mathbf{x}|\theta)$ is a joint probability density function of N independent probability density functions, $p(\mathbf{x}|\theta) = \prod_{j=1}^{N} p(x_j|\theta)$, it is often simpler to maximize the log of the likelihood function, $\ln L(\theta|\mathbf{x})$, sometimes shortened to the log-likelihood.

One controversy with maximum likelihood estimation is that $\hat{\theta}_{\text{ML}}$ does not generally satisfy the unbiased condition, Eq. (3.1). Specifically, for small N, where the estimator is much more susceptive to statistical outliers within the collected data. However, as $N \to \infty$ the estimator becomes more unbiased, $\langle \hat{\theta}_{\text{ML}} \rangle \to \theta$. The sensi-

tivity of the maximum likelihood estimator to small fluctuations in $\mathbf{x}$ is illustrated in Fig. (3.2). Additionally, the MSE of the maximum likelihood estimator tends to saturate the CRB as it becomes more unbiased [Kay93; Van00]. It is important to remark that there is no general formula to determine an appropriate value of N. However, within the framework of quantum metrology, unknown parameters are encoded into quantum resources; because of the abundance of these resources the issue of small N is often ignored.

3.1.4 Example: Biased Coin

Consider a biased coin, which when flipped results in heads with an unknown probability p_H and tails with probability $1 - p_H$. For the sake of creating a locally optimized estimator, previous coin tosses suggest that the bias is $p_H \approx p_{H,0}$. The FI of a single flip is easy to compute

$$\mathcal{I}_{\text{coin}} = \frac{1}{p_H}\Big(\frac{\partial p_H}{\partial p_H}\Big)^2 + \frac{1}{1-p_H}\Big(\frac{\partial (1-p_H)}{\partial p_H}\Big)^2 = \frac{1}{p_H(1-p_H)}, \tag{3.18}$$

thus the CRB imposes that the MSE of an unbiased estimator using N outcomes is bounded by

$$\Delta^2 \hat{p}_H \geq \frac{p_H(1-p_H)}{N}. \tag{3.19}$$

To remain somewhat general, the data collected is from N coin tosses, h of which resulted in heads and $N-h$ of which resulted in tails, which occurs with probability $\binom{N}{h} p_H^h (1-p_H)^{N-h}$. Using the locally optimized estimation strategy, Eq. (3.16), the estimator is

$$\hat{p}_H^{\text{Local}} = p_{H,0} + \frac{1}{N\mathcal{I}_{\text{coin}}} \frac{\partial \ln p_H^h (1-p_H)^{N-h}}{\partial p_H}\bigg|_{p_H \to p_{H,0}} = \frac{h}{N}, \tag{3.20}$$

which is unbiased because

$$\langle \hat{p}_H^{\text{Local}} \rangle = \sum_{h=0}^{N} \binom{N}{h} p_H^h (1-p_H)^{N-h} \frac{h}{N} = p_H. \tag{3.21}$$

Furthermore, the estimator is efficient because it saturates the CRB

$$\Delta^2 \hat{p}_H^{\text{Local}} = \sum_{h=0}^{N} \binom{N}{h} p_H^h (1-p_H)^{N-h} \Big(\frac{h}{N} - p_H\Big)^2 = \frac{p_H(1-p_H)}{N} = \frac{1}{N\mathcal{I}_{\text{coin}}}. \tag{3.22}$$

Despite the fact that the estimator was initially constructed using a local approximation, the estimator is independent of $p_{H,0}$, and is thus globally optimized. In addition, the same estimator is realized using the maximum likelihood estimation strategy, see Fig. (3.2). The biased coin exemplifies the underlying nature of the frequentist approach: as N increases, the quantity $\frac{h}{N}$ converges to the quantity p_H, from which the (albeit simple) probability density function can be reverse engineered.

3.1.5 The Bayesian Approach

The *Bayesian approach* is typically used to estimate unknown parameters which are stochastic. In other words, the latent parameters are themselves a random variable and have an intrinsic probability distribution $p(\theta)$ - which should to be confused with $p(\mathbf{x}|\theta)$. Therefore, the observed data $\mathbf{x}$ is dependent on specific realisations of θ. Consequently, a well-constructed estimator within the Bayesian approach aims to minimize the MSE for all values (global) of θ, and not subjected to local values like the frequentist approach. To achieve this, the Bayesian approach minimizes the average of a cost function $C(\hat{\theta}, \theta)$ [Kay93; TB07]

$$\langle C(\hat{\theta}, \theta) \rangle = \int p(\theta) \Big(\int p(\mathbf{x}|\theta) \big(C(\hat{\theta}(\mathbf{x}), \theta) \mathrm{d}\mathbf{x} \Big) \mathrm{d}\theta. \tag{3.23}$$

In principle, a cost function is a generalisation of the MSE for the frequentist approach. It is a function which decreases as $\hat{\theta}$ approaches θ. The MSE is an example of a cost function, so too is the absolute error $C = |\hat{\theta} - \theta|$. Different cost functions are tailored to specific probability density functions to take advantage of specific symmetries or properties.

By merging the two probability distributions, the average cost can be interpreted as an average over the simultaneous realisations of X and θ. According to Bayes' theorem (hence the name of this approach), the joint probability distribution can be interpreted in two ways

$$p(\mathbf{x}, \theta) = p(\mathbf{x}|\theta)p(\theta) = p(\theta|\mathbf{x})p(\mathbf{x}), \tag{3.24}$$

thus the average cost can be written as

$$\langle C(\hat{\theta}, \theta) \rangle = \int p(\mathbf{x}) \Big(\int \mathrm{d}\theta p(\theta|\mathbf{x}) C(\hat{\theta}(\mathbf{x}), \theta) \mathrm{d}\theta \Big) \mathrm{d}\mathbf{x}. \tag{3.25}$$

The average cost can then be minimized through standard optimization techniques, i.e by solving the equation

$$\frac{\partial}{\partial\hat{\theta}}\int p(\theta|\mathbf{x})C(\hat{\theta}(\mathbf{x}),\theta)\mathrm{d}\theta = 0, \tag{3.26}$$

where the quantity $p(\theta|\mathbf{x})$ can be computed using Bayes' theorem

$$p(\theta|\mathbf{x}) = \frac{p(\mathbf{x}|\theta)p(\theta)}{p(\mathbf{x})} = \frac{p(\mathbf{x}|\theta)p(\theta)}{\int p(\mathbf{x}|\theta)p(\theta)\mathrm{d}\theta}. \tag{3.27}$$

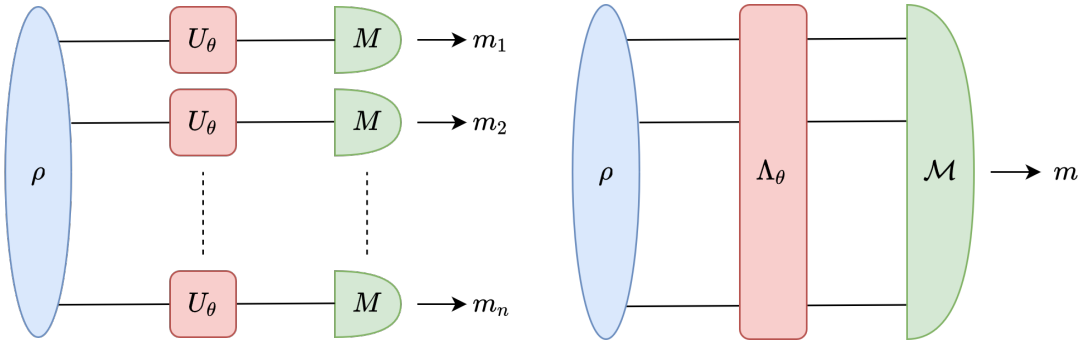
A priori knowledge of $p(\theta)$ is needed to evaluate Eq. (3.26), which is why the Bayesian approach is often used in tandem with adaptive techniques. The estimator continually outputs a new probability density function $p(\theta)$ based on the previous density function and collected data, and as the number of repetitions increases it will converge towards the correct value. There are precision bounds similar to the CRB within the Bayesian framework, but they are dependent on the cost function [BMZ87]. More information about Bayesian inference can be found in [TB07].

3.2 Quantum Estimation Theory

In the quantum setting, the foundations of the parameter estimation problem remains mostly unchanged from the classical setting [Hel69; Hol82]. An unknown parameter θ governs an n qubit quantum state ρ_θ, the individual qubits can be measured with respect to a PVM M, and the measurement outcomes $m_1,\ldots,m_n$ are used to construct an estimate $\hat{\theta}$[2]. The main difference from the classical setting is that the measurement outcomes (analogous to $\mathbf{x}$) are not necessarily independent from each other because of entanglement. As a result, estimates can be made with a super-classical precision known as the *Heisenberg limit*.

A quantum parameter estimation problem can be viewed as a two step process. The first is the 'prepare, encode and measure' step, which is inherently quantum by construction and depicted in Fig. (3.3). The second is the statistical inference step, which is uniquely classical, thus the techniques discussed in the the previous section can be applied. Therefore, using a frequentist approach with an unbiased

[2]The assumptions that the qubits are acted on independently and identically (both the encoding and the measurement) are unnecessary and impose a limit on the most general framework of a quantum parameter estimation scheme, see Fig. (3.3). These assumptions are introduced to provide a natural extension from a classical framework to a quantum framework.



(a) Phase estimation. (b) General framework.

Figure 3.3: Diagrams of the prepare, encode and measure segment of a quantum parameter estimation problem. (a) The canonical example of quantum metrology is phase estimation [GLM06], in which a phase θ is independently and identically encoded into each of the n qubits of ρ through a unitary U_θ. Each of the qubits are individually measured in accordance with a PVM M. (b) A more general framework involves θ being encoded through a general CPTP map Λ_θ, which does not necessarily act identically on the n qubits. Additionally, the PVM M is replaced by a POVM $\mathcal{M}$. The generalized setting depicted in (b) is allowable in the realm of quantum mechanics, but unlike the problem of phase estimation, it is difficult to compare to classical setting. Further, highly entangling operations and measurements are not feasible for current quantum technologies [CL01], so it is often more practical to consider the simplistic setting of phase estimation as a benchmark for quantum metrology.

estimator, if the quantum portion is repeated ν times, the MSE is bounded by a quantum version of the CRB, otherwise known as the quantum Cramér-Rao bound (QCRB)

$$\Delta^2\hat{\theta} \geq \frac{1}{\nu\mathcal{I}(\rho_\theta, \mathcal{M})} \geq \frac{1}{\nu\mathcal{Q}(\rho_\theta)}, \tag{3.28}$$

where $\mathcal{Q}$ is the quantum Fisher information (QFI), which is the FI maximized over all POVM's $\mathcal{M}$ [BC94]. Evidently, the goal of finding an optimal estimator $\hat{\theta}$ naturally divides into a classical goal and a quantum goal. The classical goal is to devise an optimal estimation technique, e.g. a locally optimized estimator or the maximum likelihood estimator, whilst the quantum goal is to find an optimal combination of initialized states ρ and POVM $\mathcal{M}$. For the task of phase estimation, this the QCRB can be saturated using highly entangled states, such as the GHZ state or NOON states, and a local measurement strategy [GLM04]. In general, the QFI is a highly non-linear equation, and there is no universal optimization strategy which is applicable to an arbitrary encoding Λ_θ. There are different mathematical techniques

to approximately solve this optimization problem [GG13; Koc+20; MBE21].

The quantum metrology schematics in Fig. (3.3) are idealized settings. In reality, it is much more complicated: environmental decoherence occurs in simultaneity with the parameter encoding, resulting in noisy measurement statistics and added uncertainty [EdMD11a; EdMD11b; DKG12]. More so, quantum technologies are not perfect, and an error may be introduced in either the quantum state preparation step or quantum measurement step. This more realistic noisy scenario is explored in greater detail in **Chapter 5**.

3.2.1 Inferring An Estimate From An Observable

A simple frequentist estimation strategy used in quantum metrology is to construct an estimator for the expectation value of an observable O and infer the value of the latent parameter from this estimate [TA14]. Assuming that O is chosen appropriately, the expectation value $\langle O \rangle = \mathrm{Tr}(O\rho_\theta)$ will be a function of θ, denoted by $f(\theta) = \mathrm{Tr}(O\rho_\theta)$. An estimate of $f(\theta)$, $\hat{f}$, can be inverted to obtain $\hat{\theta} = f^{-1}(\hat{f})$. The estimator $\hat{f}$ is designed using the frequentist philosophy: with sufficient data $\nu \gg 1$, the frequency of the measurement results will mimic the true probability density function. Denote the eigenvalues of O as $\{\lambda_j\}$ with corresponding eigenvectors $\{|\phi_j\rangle\}$

$$O = \sum_j \lambda_j \left|\phi_j\right\rangle\!\left\langle\phi_j\right| . \tag{3.29}$$

The state ρ_θ is measured with respect to the eigenbasis of O. The results are recorded as $m_1, \ldots, m_\nu$: if the kth measurement results in $|\phi_j\rangle$, then $m_k = \lambda_j$ and the maximum likelihood estimate can be written as

$$\hat{f} = \frac{1}{\nu} \sum_{k=1}^{\nu} m_k. \tag{3.30}$$

This is an unbiased estimate because

$$\mathbb{E}(\hat{f}) = \frac{1}{\nu} \sum_{k=1}^{\nu} \mathbb{E}(m_k) = \frac{1}{\nu} \sum_{k=1}^{\nu} \sum_j \lambda_j \,\mathrm{Tr}(\rho_\theta \left|\phi_j\right\rangle\!\left\langle\phi_j\right|) = \frac{1}{\nu} \sum_{k=1}^{\nu} \langle O \rangle = \langle O \rangle , \tag{3.31}$$

and the MSE is proportional to the variance of O

$$\Delta^2 \hat{f} = \frac{\Delta^2 O}{\nu} = \frac{\mathrm{Tr}(O^2\rho_\theta) - \mathrm{Tr}(O\rho_\theta)^2}{\nu}. \tag{3.32}$$

An issue with this estimation technique is that $f(\theta)$ is not necessarily an invertible function, and thus $\hat{f} = f^{-1}(\hat{f})$ may be ambiguous. That is of course, unless one has a priori knowledge of $\theta \approx \theta_0$ such that one can properly define a local inverse in the region surrounding $f(\theta_0)$. Assuming this is true and that the MSE is small, $\Delta^2 \hat{f} \ll 1$, then by the central limit theorem $\hat{f}$ fluctuates close to $\langle O \rangle$, validating the first order Taylor approximation

$$\hat{\theta} = f^{-1}(\hat{f}) \approx f^{-1}(\langle O \rangle) + \frac{\partial f^{-1}(\hat{f})}{\partial \hat{f}}\Big|_{\hat{f} \to \langle O \rangle} (\hat{f} - \langle O \rangle) = \theta + \frac{1}{\frac{\partial \langle O \rangle}{\partial \theta}} (\hat{f} - \langle O \rangle). \tag{3.33}$$

It follows from the above approximation that the estimator $\hat{\theta}$ is unbiased and has MSE

$$\Delta^2 \hat{\theta} = \frac{\Delta^2 \hat{f}}{|\frac{\partial \langle O \rangle}{\partial \theta}|^2} = \frac{\Delta^2 O}{\nu |\frac{\partial \langle O \rangle}{\partial \theta}|^2}. \tag{3.34}$$

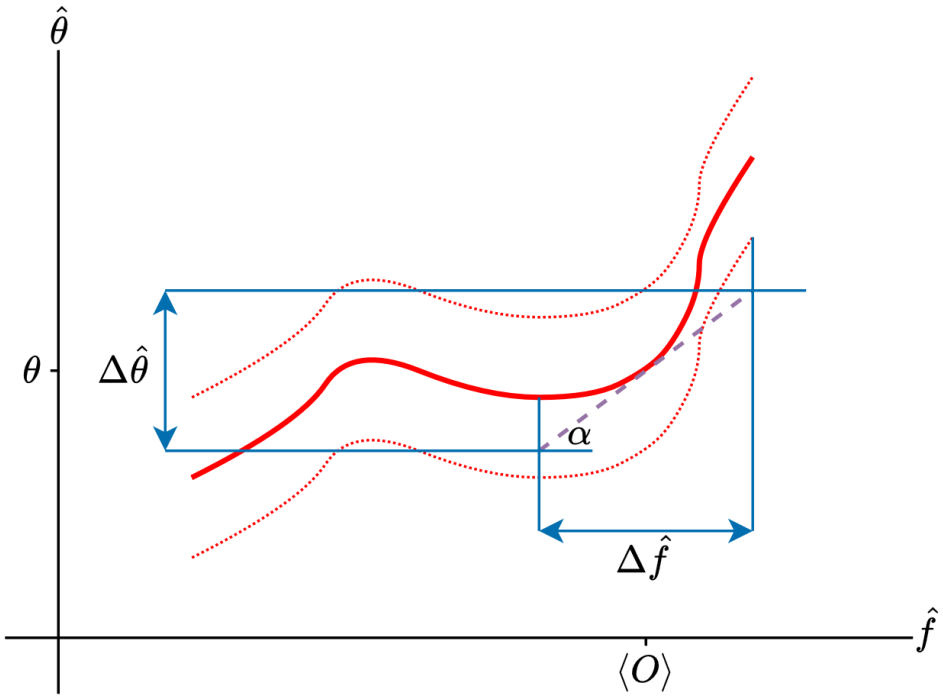


Figure 3.4: Graphical calculation of the MSE $\Delta^2 \hat{\theta}$ using the error propagation formula. The solid red curve depicts $\hat{\theta} = f^{-1}(\hat{f})$, which at the point $\hat{f} \to \langle O \rangle$ has a tangent with angle α, therefore, $\frac{\Delta \hat{\theta}}{\Delta \hat{f}} = |\tan \alpha| = |\frac{\partial \langle O \rangle}{\partial \theta}|^{-1}$.

Eq. (3.34) is the error propagation formula, which quantifies the amount that $\hat{\theta}$ fluctuates around θ in terms of the fluctuations of $\hat{f}$ around $\langle O \rangle$ [Ku+66]. A geomet-

ric intuition of the formula is depicted in Fig. (3.4). The term in the denominator $|\frac{\partial\langle O\rangle}{\partial\theta}|^2$ encapsulates the difficulty of inverting a function when there is uncertainty. The effects of uncertainty are amplified near a local maxima or minima, but diminish as $|\frac{\partial\langle O\rangle}{\partial\theta}| \to \infty$.

3.2.2 Quantum Fisher Information

Using the semantics of quantum information theory, the explicit expression for the FI with respect to a POVM $\mathcal{M}$ with outcomes $\{E_m\}$ can be written as

$$\mathcal{I}(\rho_\theta, \mathcal{M}) = \int \frac{\big(\operatorname{Tr}(E_m \dot{\rho}_\theta)\big)^2}{\operatorname{Tr}(E_m \rho_\theta)} \mathrm{d}m, \tag{3.35}$$

where the notation $\dot{\square} = \frac{\partial \square}{\partial \theta}$ is used for conciseness. Just as the FI is interpreted as an information measure, so too is the QFI [BG00]. Eq. (3.12) suggests that the POVM which maximizes the distinguishability between the probability density functions associated to ρ_θ and $\rho_{\theta+\delta\theta}$ will similarly maximize the FI. This is a principle idea behind the derivation of the closed form expression of the QFI [BC94].

The derivation begins by defining the superoperator

$$\mathcal{R}_{\rho_\theta}(O) = \frac{1}{2}(\rho_\theta O + O\rho_\theta), \tag{3.36}$$

whose inverse[3] is

$$\mathcal{R}^{-1}_{\rho_\theta}(O) = \sum_{j,k} \frac{2}{\lambda_j + \lambda_k} O_{jk} \left|j\right\rangle\!\left\langle k\right|, \tag{3.37}$$

where $\rho_\theta = \sum_j \lambda_j \left|j\right\rangle\!\left\langle j\right|$ is the orthonormal expansion of ρ_θ and $O_{jk} = \langle j|O|k\rangle$. A property of $\mathcal{R}$ is that for any Hermitian A and B, $\operatorname{Tr}\big(AB\big) = \operatorname{Re}\big[\operatorname{Tr}\big(\rho_\theta A \mathcal{R}^{-1}_{\rho_\theta}(B)\big)\big]$, from which it follows that the FI can be written as

$$\begin{aligned}
\mathcal{I}(\rho_\theta, \mathcal{M}) &= \int \frac{\operatorname{Re}\big[\operatorname{Tr}\big(\rho_\theta E_m \mathcal{R}^{-1}_{\rho_\theta}(\dot{\rho}_\theta)\big)\big]^2}{\operatorname{Tr}(E_m \rho_\theta)} \mathrm{d}m \\
&\leq \int \frac{\big|\operatorname{Tr}\big(\rho_\theta E_m \mathcal{R}^{-1}_{\rho_\theta}(\dot{\rho}_\theta)\big)\big|^2}{\operatorname{Tr}(E_m \rho_\theta)} \mathrm{d}m \\
&= \int \frac{\big|\operatorname{Tr}\big(\sqrt{\rho_\theta}\sqrt{E_m}\sqrt{E_m}\mathcal{R}^{-1}_{\rho_\theta}(\dot{\rho}_\theta)\sqrt{\rho_\theta}\big)\big|^2}{\operatorname{Tr}(E_m \rho_\theta)} \mathrm{d}m.
\end{aligned} \tag{3.38}$$

[3]The inverse $\mathcal{R}^{-1}_{\rho_\theta}(O)$ is not always well defined for all O, however the quantity used in the derivation of the QFI, $\mathcal{R}^{-1}_{\rho_\theta}(\dot{\rho}_\theta)$, always converges to a well-defined Hermitian operator.

The final step in the derivation uses the Cauchy-Schwarz inequality $|\operatorname{Tr}(A^\dagger B)|^2 \leq \operatorname{Tr}(AA^\dagger)\operatorname{Tr}(BB^\dagger)$ with $A = \sqrt{E_m}\sqrt{\rho_\theta}$ and $B = \sqrt{E_m}\mathcal{R}_{\rho_\theta}^{-1}(\dot{\rho}_\theta)\sqrt{\rho_\theta}$,

$$\begin{aligned}\mathcal{I}(\rho_\theta, \mathcal{M}) &\leq \int \operatorname{Tr}\left(E_m \mathcal{R}_{\rho_\theta}^{-1}(\dot{\rho}_\theta)\rho_\theta \mathcal{R}_{\rho_\theta}^{-1}(\dot{\rho}_\theta)\right)\mathrm{d}m \\ &= \operatorname{Tr}\left(\mathcal{R}_{\rho_\theta}^{-1}(\dot{\rho}_\theta)\rho_\theta \mathcal{R}_{\rho_\theta}^{-1}(\dot{\rho}_\theta)\right) \\ &= \mathcal{Q}(\rho_\theta).\end{aligned} \tag{3.39}$$

The Hermitian operator $\mathcal{R}_{\rho_\theta}^{-1}(\dot{\rho}_\theta)$ is the symmetric logarithmic derivative. The QCRB can be saturated by setting $\mathcal{M}$ to be the measurement in the eigenbasis of $\mathcal{R}_{\rho_\theta}^{-1}(\dot{\rho}_\theta)$ [BC94; Luo00; Mat02]. Unfortunately, but not surprisingly, such a measurement is encumbered by the usual quandary of the frequentist approach: the measurement basis is dependent on θ[4]. Furthermore, this measurement strategy is very sophisticated and out of reach for current technologies [CL01]. Fortunately, this is not the unique measurement strategy which saturates the QCRB [GLM04]. As mentioned, the quantum goal of parameter estimation problems is to determine feasible measurement schemes which best saturate the QCRB.

A closed form expression for the QFI can be derived using the definition of $\mathcal{R}_{\rho_\theta}^{-1}(\dot{\rho}_\theta)$, Eq. (3.37),

$$\mathcal{Q}(\rho_\theta) = \sum_j \frac{\dot{\lambda}_j^2}{\lambda_j} + 2\sum_{j,k} \frac{(\lambda_j - \lambda_k)^2}{\lambda_j + \lambda_k} |\langle \dot{j} | k \rangle|^2. \tag{3.40}$$

The first sum is reminiscent of the classical FI and quantifies the amount of extractable information from the eigenvalues $\{\lambda_j\}$. Whilst the second sum accounts for quantum effects such as superposition and entanglement and quantifies the amount of extractable information from the quantum states $\{|j\rangle\}$. To a certain extent, the classical term is limited to 'amplitudes', while the quantum term has access to 'amplitudes' and 'phases'. As such, the quantum term is significantly more influential than the classical term, this is reinforced by the convexity property of the QFI [AR15]

$$\mathcal{Q}\big(p\rho_1 + (1-p)\rho_2\big) \leq p\mathcal{Q}(\rho_1) + (1-p)\mathcal{Q}(\rho_2). \tag{3.41}$$

For the special case of pure states $\rho_\theta = |\psi_\theta\rangle\langle\psi_\theta|$, the expression is much more aesthetically pleasing. It follows from $\rho_\theta^2 = \rho_\theta$ that $\dot{\rho}_\theta = \rho_\theta\dot{\rho}_\theta + \dot{\rho}_\theta\rho_\theta$ and thus $\mathcal{R}_{\rho_\theta}^{-1}(\dot{\rho}_\theta) = 2\dot{\rho}_\theta$.

[4] Similar to how a locally optimized estimator, Eq. (3.16), approximately saturates the CRB, measuring in the eigenbasis of $\mathcal{R}_{\rho_\theta}^{-1}(\dot{\rho}_\theta)|_{\theta\to\theta_0}$ approximately saturates the QCRB.

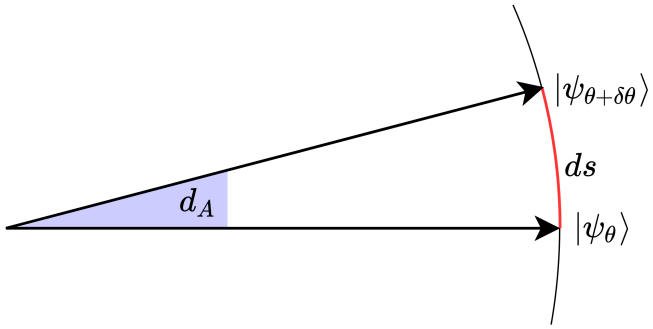


Figure 3.5: The length of the chord between $|\psi_\theta\rangle$ and $|\psi_{\theta+\delta\theta}\rangle$ is $2\sin\frac{d_A}{2}$. For small d_A, the length of the chord is approximately equal to the length of the geodesic, $ds \approx 2\sin\frac{d_A}{2} \approx d_A$. This idea generalizes to higher dimensional abstract surfaces $\mathbb{CP}^n$ as well as their interior points (mixed states).

The QFI simplifies greatly to

$$\mathcal{Q}(|\psi_\theta\rangle) = 4\,\mathrm{Tr}\big(\rho_\theta \dot{\rho}_\theta^2\big) = 4\big(\langle\dot{\psi}_\theta|\dot{\psi}_\theta\rangle - |\langle\dot{\psi}_\theta|\psi_\theta\rangle|^2\big). \tag{3.42}$$

In fact, it was shown that a similar expression holds for arbitrary mixed states [EdMD11b]

$$\mathcal{Q}(\rho_\theta) = \min_{|\Psi_\theta\rangle} 4\big(\langle\dot{\Psi}_\theta|\dot{\Psi}_\theta\rangle - |\langle\dot{\Psi}_\theta|\Psi_\theta\rangle|^2\big), \tag{3.43}$$

where the minimization is taken over all possible purifications, Eq. (2.10), of ρ_θ.

3.2.3 Geometric Perspectives Of The QFI

The representation introduced in **Chapter 2** is that a quantum state $|\psi\rangle$ can be thought of as a vector which is an element of a Hilbert space $\mathcal{H}$. An alternative to this is a geometric representation, where n qubit quantum states are thought to be elements of the complex projective space $\mathbb{CP}^n$ [Woo81; PS96; GKM05]. Pure states reside on the surface of this Riemannian manifold and mixed states in the interior, the $n = 1$ case is the well-known Bloch sphere portrayed in Fig. (2.1). $\mathbb{CP}^n$ is equipped with an infinitesimal metric called the Fubini-Study metric ds^2, which is called the Bures metric [Bur69; SZ03] when it is extended to include the interior. Such a metric allows one to compare neighbouring quantum states ρ_θ and $\rho_{\theta+\delta\theta}$, analogous to the FI metric for (classical) statistical manifolds, it can be shown that $ds^2 = \frac{1}{4}\mathcal{Q}(\rho_\theta)\delta\theta^2$ [Fac+10; SK20].

The Bures angle d_A is the angle between the rays of ρ_1 and ρ_2, explicitly [Ama16;

BŻ17]

$$d_A(\rho_1, \rho_2) = \arccos \sqrt{\mathscr{F}(\rho_1, \rho_2)}, \tag{3.44}$$

where $\mathscr{F}$ is the fidelity, Eq. (2.34). For neighbouring quantum states, the Bures angle can be approximated two different ways. The first way is by using a first order Taylor expansion

$$d_A(\rho_\theta, \rho_{\theta+\delta\theta}) = \sqrt{2 - 2\sqrt{\mathscr{F}(\rho_\theta, \rho_{\theta+\delta\theta})}} + \mathcal{O}(\delta\theta^2). \tag{3.45}$$

The second is a geometric approximation using the Bures metric (and by extension the QFI), the intuition of which is given in Fig. (3.5)

$$d_A(\rho_\theta, \rho_{\theta+\delta\theta}) = ds + \mathcal{O}(\delta\theta^2) = \frac{1}{2}\sqrt{\mathcal{Q}(\rho_\theta, \rho_{\theta+\delta\theta})}\delta\theta + \mathcal{O}(\delta\theta^2). \tag{3.46}$$

A new expression for the QFI is obtained by merging the two equations [SK20]

$$\mathcal{Q}(\rho_\theta) = \lim_{\delta\theta\to 0} 8\frac{1 - \sqrt{\mathscr{F}(\rho_\theta, \rho_{\theta+\delta\theta})}}{\delta\theta^2}, \tag{3.47}$$

which can be useful to derive analytic bounds for the QFI and other information theoretic quantities [Suz19; TAD20]. A corollary of Eq. (3.47) is the concavity of the QFI under CPTP maps $\mathcal{E}$

$$\mathcal{Q}\big(\mathcal{E}(\rho_\theta)\big) \leq \mathcal{Q}\big(\rho_\theta\big), \tag{3.48}$$

which follows from the monotonicity of the fidelity $\mathscr{F}\big(\mathcal{E}(\rho_1), \mathcal{E}(\rho_2)\big) \geq \mathscr{F}\big(\rho_1, \rho_2\big)$. If $\mathcal{E}$ is thought of as an interaction with an environment (**Chapter 5**) or a malicious adversary (**Chapter 6**), then the concavity of the QFI can be understood as information about θ being lost to these outside sources.

3.2.4 Ultimate Precision: The Heisenberg Limit

To recapitulate: the CRB is a bound on the MSE by optimizing over estimation strategies, and the QCRB extends the bound by optimizing over measurement strategies. The next natural extension is to optimize over initialized quantum states, to find the true limit of precision attainable through quantum mechanics. The upper bound for which is referred to as the *Heisenberg Limit* (HL) [YMK86; HB93].

Originally, the HL was derived within the framework of phase estimation. In the phase estimation problem, a phase θ is encoded into each qubit of an n qubit pure

state $|\psi\rangle$ by a unitary $U_\theta = e^{-i\theta H}$, where the Hamiltonian H acts independently and identically on all n qubits. The QFI can be calculated to be

$$\mathcal{Q} = 4\big(\langle\psi|H^2|\psi\rangle - |\langle\psi|H|\psi\rangle|^2 \big) = 4\Delta^2 H. \tag{3.49}$$

The etymology of the term 'Heisenberg limit' stems from the fact that the QCRB (with $\nu = 1$) can be manipulated to mimic the the Heisenberg uncertainty principle

$$\Delta^2\hat{\theta}\Delta^2 H \geq \frac{1}{4}. \tag{3.50}$$

The QFI for phase estimation can be maximized by setting $|\psi\rangle$ to be a highly entangled state, such as the GHZ state for qubit systems or the NOON state for photonic systems, which results in $\mathcal{Q} = n^2$. Hence, the ultimate allowable precision by quantum mechanics (the HL) is

$$\Delta^2\hat{\theta}_{\mathrm{HL}} = \frac{1}{\nu n^2}. \tag{3.51}$$

The HL offers a quadratic improvement compared to the standard quantum limit (SQL), where the $|\psi\rangle$ is limited to separable states

$$\Delta^2\hat{\theta}_{\mathrm{SQL}} = \frac{1}{\nu n}. \tag{3.52}$$

The SQL is also referred to as the classical limit or the shot-noise limit [XWK87].

For qubit (and qudit) systems[5], entanglement is a crucial resource for quantum metrology [PS09; Pez+18]. In fact, the quadratic tendencies of the QFI of a quantum state for phase estimation can be bounded with respect to the geometric measure of entanglement G[6] [Aug+16]

$$\mathcal{Q}(\rho_\theta) \leq n + 8n^2\sqrt{G(\rho_\theta)}. \tag{3.53}$$

It is worth stressing that entanglement may be a necessary condition to surpass the SQL but it is not a sufficient condition [HGS10; Osz+16]. Additionally, the bounds in Eq. (3.51) and Eq. (3.52) are exclusive to the problem of phase estimation with an iid encoding. The QFI can surpass n^2 for non-linear H [Lui04; Boi+07; CS08;

[5]For CV systems a quantum advantage can be achieved with squeezing [YMK86; OH10].

[6]The geometric measure of entanglement for a pure state $|\psi\rangle$ is $G(|\psi\rangle) = 1 - \max_{|\phi\rangle} |\langle\phi|\psi\rangle|^2$, where $|\phi\rangle$ is maximized over all fully separable states. The definition is extended to mixed states by finding the convex roof of the geometric measure of entanglement over all possible statistical ensembles [WG03].

Bra+18], and scenarios can be devised in which entanglement is not a necessary resource [Til+10].

3.2.5 Bayesian Approach To Quantum Metrology

In the quantum version of the frequentist approach, the MSE is minimized by optimizing over all possible POVM's and input quantum states. The quantum version of the Bayesian approach [Hol82; JD15; RKD18] is enhanced in an analogous fashion. As the estimator is updated adaptively, so too can the initialized quantum state as well as choice of POVM.

For parameter estimation problems which exhibit periodicity, such as phase estimation, the circular cost function

$$C_\circ(\hat{\theta}, \theta) = 4\sin^2\left(\frac{\hat{\theta} - \theta}{2}\right) \tag{3.54}$$

is a natural choice as a figure of merit [Dem11; DJK15], and converges to the MSE as $\hat{\theta}$ approaches θ. If the initial choice of input quantum state and POVM are $\rho_\theta = U_\theta \rho_0 U_\theta^\dagger$ and $\int E_m \mathrm{d}m$ respectively, then the average cost is

$$\langle C_\circ \rangle = \int p(\theta) \left(\int \mathrm{Tr}(\rho_\theta E_m) C_\circ(\hat{\theta}(m), \theta) \mathrm{d}m \right) \mathrm{d}\theta, \tag{3.55}$$

which is invariant when replacing the POVM $\{E_m\}$ with a covariant POVM $\{E_{\hat{\theta}}\}$ [Hol82; DBE98; Chi+04; CDS05]

$$E_{\hat{\theta}} = U_{\hat{\theta}} \Sigma U_{\hat{\theta}}^\dagger \tag{3.56}$$

and Σ is the positive-semi definite operator defined for a specific $\hat{\theta}$

$$\Sigma = \int U_{\hat{\theta}(m)}^\dagger E_m U_{\hat{\theta}(m)} \mathrm{d}m. \tag{3.57}$$

This re-parametrization allows the average cost to be expressed as

$$\begin{aligned} \langle C_\circ \rangle &= \int \int p(\theta) \, \mathrm{Tr}(\rho_\theta E_{\hat{\theta}}) C_\circ(\hat{\theta}, \theta) \mathrm{d}\hat{\theta} \mathrm{d}\theta \\ &= \int p(\theta) \, \mathrm{Tr}(\rho_\theta \Sigma) 4\sin^2 \frac{\theta}{2} \mathrm{d}\theta. \end{aligned} \tag{3.58}$$

By optimizing the above expression, the initialized quantum state ρ_0 and POVM

characterized by Σ can be updated adaptively [DBE98; CDS05].

As mentioned, the Bayesian statistical inference approach addresses the issues inherent to the frequentist approach: lack of a priori knowledge [KD10; Dem11] and limited resources [RD20]. The work presented in the subsequent chapters exclusively focus on the frequentist approach, as such, an interesting future perspective would be to generalize some of the findings to the Bayesian approach. Specifically in **Chapter 6**, where the estimation process is adapted in some capacity to account for the cryptographic framework.

3.2.6 Multiple Parameters

In the interest of simplicity, this chapter introduced the problem of parameter estimation with a single unknown parameter. The problem naturally generalizes to include multiple latent parameters $\theta \to \boldsymbol{\theta} = \{\theta_1, \ldots, \theta_m\}$, where the goal extends to devising estimators for each parameter $\hat{\theta}(\mathbf{x}) \to \hat{\boldsymbol{\theta}}(\mathbf{x}) = \{\hat{\theta}_1(\mathbf{x}), \ldots, \hat{\theta}_m(\mathbf{x})\}$. There are two major quandaries which arise in the multiparameter setting. First, the parameters may be statistically dependent on one another, which adds ambiguity when trying to interpret the observed data $\mathbf{x}$. Second, it is not always possible to simultaneously construct an efficient estimator for each unknown parameter.

Within the frequentist inference framework, assuming that each estimator satisfies the unbiased estimator constraint, $\mathbb{E}(\hat{\boldsymbol{\theta}}) = \boldsymbol{\theta}$, the generalization of the QCRB is the matrix equation [YL73; HK74; TWC11]

$$\mathbf{Cov}(\boldsymbol{\theta}) \geq \frac{1}{\nu}\boldsymbol{\mathcal{I}}^{-1}(\boldsymbol{\theta}) \geq \frac{1}{\nu}\boldsymbol{\mathcal{Q}}^{-1}(\boldsymbol{\theta}), \tag{3.59}$$

where $\mathbf{Cov}(\boldsymbol{\theta})$ is the covariance matrix with entries $\mathbf{Cov}(\boldsymbol{\theta})_{i,j} = \langle(\hat{\theta}_i - \theta_i)(\hat{\theta}_j - \theta_j)\rangle$, $\boldsymbol{\mathcal{I}}(\boldsymbol{\theta})$ is the FI matrix

$$\boldsymbol{\mathcal{I}}(\boldsymbol{\theta})_{i,j} = \int p(\mathbf{x}|\boldsymbol{\theta})\Big(\frac{\partial \ln p(\mathbf{x}|\boldsymbol{\theta})}{\partial\theta_i}\Big)\Big(\frac{\partial \ln p(\mathbf{x}|\boldsymbol{\theta})}{\partial\theta_j}\Big)\mathrm{d}\mathbf{x}, \tag{3.60}$$

and $\boldsymbol{\mathcal{Q}}(\boldsymbol{\theta})$ is the QFI matrix

$$\boldsymbol{\mathcal{Q}}(\boldsymbol{\theta})_{i,j} = \mathrm{Tr}\left(\mathcal{R}_{\rho_{\boldsymbol{\theta}}}^{-1}\big(\frac{\partial\rho_{\boldsymbol{\theta}}}{\partial\theta_i}\big)\rho_{\boldsymbol{\theta}}\mathcal{R}_{\rho_{\boldsymbol{\theta}}}^{-1}\big(\frac{\partial\rho_{\boldsymbol{\theta}}}{\partial\theta_j}\big)\right). \tag{3.61}$$

The diagonal elements of an invertible positive semi-definite matrix M satisfy $M_{i,i} \geq 1/M_{i,i}$, and equality holds for each i when M is diagonal. Hence, when the m pa-

rameters are statistically independent from each other, Eq. (3.59) reduces to the QCRB for each individual parameter θ_i. Multiparameter estimation sustains additional complications in the quantum context with respect to optimizing quantum states and measurements. The superoperator $\mathcal{R}_{\rho_{\boldsymbol{\theta}}}^{-1}\left(\frac{\partial \rho_{\boldsymbol{\theta}}}{\partial \theta_i}\right)$ is the symmetric logarithmic derivative with respect to θ_i, and measuring in all of these bases will saturate the QCRB. However, these measurements may not be compatible and thus cannot be realized in simultaneity [Vid+14; Cro+14; RJD16].

Despite the additional complexity of simultaneously estimating multiple parameters, multiparameter quantum metrology is an active research topic [SBD16; Nic+18; AFD19; RD20; MBE21]. With respect to phase estimation, when the phase encoding unitaries do not commute, it is more efficient to estimate them in simultaneity rather than independently [BD16]; when the encoding unitaries do commute, one can devise a simultaneous estimation strategy which is at least as efficient as estimating the phases independently [Hum+13]. Multiparameter quantum metrology is a natural framework for eigenvalue estimation of higher dimensional unitaries [Fuj01; Bal04; Ber+15; BD16] and for spatially distributed estimation problems [Eld+18; Ge+18; PKD18; ZZS18; Rub+20; Guo+20]. The subsequent research chapters focus on the single parameter setting. Nonetheless, the mathematical techniques and derivations can easily be adapted to the multiple parameter setting. Formally addressing these generalizations is a future perspective of the works presented.

3.3 Example Applications Of Quantum Metrology

The final section of this chapter explores well-known applications of quantum metrology where the concepts and tools that were introduced are put into practise. The examples chosen, phase estimation and amplitude estimation, have a simple mathematical formalism and highlight the novelty of a quantum parameter estimation problem. Specifically, phase estimation, which is indisputably the canonical usage of quantum metrology [Cav81; GLM04], clearly showcases the advantages a quantum system can provide. Additionally, phase estimation is the core problem of **Chapter 4** and **Chapter 5**. The example of amplitude estimation, although not present in the subsequent research chapters, is included to showcase a simple usage which is not phase estimation.

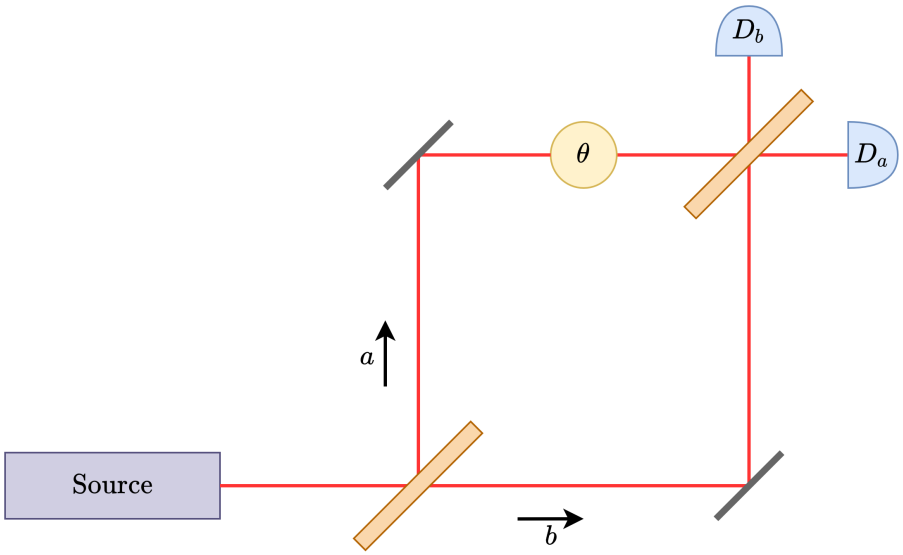


Figure 3.6: Schematic of a Mach-Zehnder interferometer. A photonic source is fired onto a 50:50 beam splitter, which reflects a photon with 50% probability (path a), otherwise the photon is transmitted (path b). A phase shift of θ is introduced uniquely on path a, after the paths interfere via a second beam splitter. The quantum state is measured with photon-counters, whose outcomes j are dependent on the relative phase θ.

3.3.1 Phase Estimation (Photonic Interferometry)

Phase estimation is a benchmarking problem for quantum metrology [HB93]. It encapsulates a variety of applications for quantum sensors, notably magnetometry [Tay+08; Was+10; Sew+12; BCK15; Raz+19], frequency estimation for optomechanical sensors [ZYL16; DPD19; Tsa13], spectroscopy [Mey+01; Lei+04; Kir+11; DSM16; Sha+18] and unitary tomography [SHF13; OTT19]. The premise of phase estimation is simple, yet the results are an elegant display of a quantum advantage. A relative phase is encoded into a quantum system via a physical interaction, and using highly entangled states and a simple measurement strategy, the QCRB can be saturated to attain the HL [GLM06].

For photonic sources, a relative phase can be introduced using a Mach-Zehnder interferometer [ZAT00], depicted in Fig. 3.6. A photonic quantum state passes through a 50:50 beam splitter, in which photons are either transmitted or reflected, both with probability of one half, where reflection induces a phase shift of $\pi/2$ [Dow08]. After passing through the first beam splitter, a single photon will be in a superposition of the two possible modes, labelled by the respective paths $|a\rangle$ and $|b\rangle$.

Since photons are indistinguishable particles, it is customary to write an n photon quantum state as

$$|\psi\rangle = \sum_{k=0}^{n} \alpha_k \, |k, n-k\rangle \, , \tag{3.62}$$

where the notation $|k, n-k\rangle$ denotes the quantum state with k photons in mode $|a\rangle$ and $n-k$ photons in mode $|b\rangle$. The path-dependent phase shift is represented by the unitary

$$U_\theta = \exp\Big(-i \frac{\theta}{2} \big(\, |a\rangle\langle a| - |b\rangle\langle b| \, \big) \Big)^{\otimes n} , \tag{3.63}$$

thus

$$U_\theta \, |k, n-k\rangle = e^{-i\frac{2k-n}{2}\theta} \, |k, n-k\rangle \, . \tag{3.64}$$

After the phase shifts, the two paths interfere by passing through a second beam splitter. This causes the detection probabilities to be dependent on θ, from which the statistics can be used to generate an estimate $\hat{\theta}$. The precision of the estimate is ultimately bounded by the QFI

$$\mathcal{Q}(|\psi\rangle) = \sum_{k=0}^{n} |\alpha_k|^2 (2k-n)^2 - \Big(\sum_{k=0}^{n} |\alpha_k|^2 (2k-n) \Big)^2 = 4 \sum_{k=0}^{n} |\alpha_k|^2 k^2 - 4 \Big(\sum_{k=0}^{n} |\alpha_k|^2 k \Big)^2 . \tag{3.65}$$

Suppose that the source of photons is uncorrelated such that the quantum state after passing through the first beam splitter is

$$|\psi\rangle_{\text{sep}} = \frac{1}{\sqrt{2^n}} \Big(\, |a\rangle + |b\rangle \, \Big)^{\otimes n} = \sum_{k=0}^{n} \sqrt{2^{-n} \binom{n}{k}} \, |k, n-k\rangle \, . \tag{3.66}$$

Using Eq. (3.65), the QFI can be computed to be equal to the SQL, $\mathcal{Q}_{\text{sep}} = n$. In contrast, if the quantum state is initialized in the NOON state [Dow08; Mat+16; ZC18]

$$|\psi\rangle_{\text{ent}} = \frac{1}{\sqrt{2}} \Big(\, |n, 0\rangle + |0, n\rangle \, \Big) , \tag{3.67}$$

then the HL is attained[7], $\mathcal{Q}_{\text{ent}} = n^2$. The QCRB can be saturated using the previously described method of inferring an estimate from an observable. The chosen observable is the parity of the detected photons in detector a, labelled D_a in, Fig. 3.6,

$$O_{\text{parity}} = \sum_{k=0}^{n} (-1)^k \, |k, n-k\rangle\langle k, n-k| \, . \tag{3.68}$$

[7] This has been experimentally accomplished using $n = 4$ photons [Nag+07]

Assuming no dark counts, if D_a detects j photons, D_b is fixed to $n-j$ photons, hence the parity of D_b could have equally been considered. After intercepting the second beam splitter, the quantum state (up to a global phase) is

$$\begin{aligned} |\psi_\theta\rangle_{\text{ent}} &= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{n} \sqrt{\binom{n}{k}} \left(e^{-in\theta/2} i^{n-k} + e^{in\theta/2} i^k \right) |k, n-k\rangle \\ &= \frac{1}{\sqrt{2^{n-1}}} \sum_{k=0}^{n} \sqrt{\binom{n}{k}} \cos\left(\frac{n\theta}{2} + \frac{\pi}{4}(2k-n) \right) |k, n-k\rangle \,, \end{aligned} \tag{3.69}$$

from which it can be computed that

$$\langle O \rangle_{\text{ent}} = \cos\left(n\theta - \frac{\pi n}{2} \right). \tag{3.70}$$

If the prepare and measure protocol is repeated ν times, the MSE of the estimator is

$$\Delta^2 \hat{\theta}_{\text{ent}} = \frac{\Delta^2 O_{\text{ent}}}{\nu \left| \frac{\partial \langle O \rangle_{\text{ent}}}{\partial \theta} \right|^2} = \frac{1}{\nu n^2}, \tag{3.71}$$

thus the QCRB is saturated with a simple measurement strategy. This example highlights the achievability of a quantum advantage, but simultaneously the locality of the frequentist approach. The periodicity of $\langle O \rangle_{\text{ent}}$ implies that a priori knowledge of θ is required to an order of $2\pi/n$. If θ is completely unknown, a frequentist approach can still be employed using varying $n = 2^m$, where successive rounds of estimation are used to estimate the mth (binary) digit of θ [Kit95].

In this example, a relative phase is encoded using a photonic source by means of a Mach-Zehnder interferometer. Notably though, analogous results are obtained using spin systems [TA14]. In fact, the NOON state, Eq. (3.67), can be interpreted as a GHZ state

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}} (|0\rangle^{\otimes n} + |1\rangle^{\otimes n}), \tag{3.72}$$

which when used for phase estimation, similarly saturates the HL.

3.3.2 Amplitude Estimation (Thermometry)

After phase estimation, the next obvious example of a quantum metrology problem is amplitude estimation. A well-known example of amplitude estimation is quantum thermometry [Cor+15; DS18; MSC19], where the unknown parameter in question is temperature. Temperature is a seemingly intuitive notion ever present in our daily

lives, and measuring this quantity may appear trivial. For every day objects, an infra-red thermometer converts infra-red radiation into a voltage which is converted into a temperature. This is done extremely quickly and accurately. Even so, in the 'very cold' regime near zero Kelvin, measuring temperature is a complicated task, but very necessary for modern technologies such as superconductors.

Even though experimental implementations of quantum thermometry differ greatly [Neu+13; Toy+13; Kuc+13], the underlying principle is straightforward [MSC19]. An N level system interacts with an external source at temperature T. Eventually, the collective ensemble of the system and the bath will reach thermal equilibrium, and the state of the system is given by the Gibbs ensemble

$$\rho_T = \frac{1}{Z} e^{-\frac{H}{k_B T}}, \tag{3.73}$$

where k_B is the Boltzmann constant, H is the system Hamiltonian

$$H = \sum_{k=1}^{N} \epsilon_k \, |\epsilon_k\rangle\langle\epsilon_k| \tag{3.74}$$

with energy eigenvalues ϵ_k and eigenstates $|\epsilon_k\rangle$, and $Z = \operatorname{Tr} e^{-\frac{H}{k_B T}}$ is the partition function. Within the standard convention of setting $k_B = 1$, the derivative of the quantum system with respect to temperature is

$$\dot{\rho}_T = \frac{H}{T^2}\rho_T - \frac{\langle H\rangle}{T^2}\rho_T = \frac{1}{2T^2}\big((H - \langle H\rangle)\rho_T + \rho_t(H - \langle H\rangle)\big). \tag{3.75}$$

From which it is clear that the symmetric logarithmic derivative is

$$\mathcal{R}_{\rho_T}^{-1}(\dot{\rho}_T) = \frac{1}{T^2}(H - \langle H\rangle), \tag{3.76}$$

therefore

$$\mathcal{Q}(\rho_T) = \operatorname{Tr}\left(\mathcal{R}_{\rho_T}^{-1}(\dot{\rho}_T)\rho_T\mathcal{R}_{\rho_T}^{-1}(\dot{\rho}_T)\right) = \frac{1}{T^4}\operatorname{Tr}\left((H - \langle H\rangle)^2\rho_T\right) = \frac{\Delta^2 H}{T^4}. \tag{3.77}$$

In fact, the heat capacity

$$\frac{\partial\langle H\rangle}{\partial T} = \frac{\Delta^2 H}{T^2} \tag{3.78}$$

is directly proportional to the QFI [Phi84], hence the QCRB can be re-written as

$$\Delta^2\hat{T} \geq \frac{1}{\nu\mathcal{Q}} = \frac{\Delta^2 H}{\nu|\frac{\partial\langle H\rangle}{\partial T}|^2}. \tag{3.79}$$

Which suggests that the QCRB can be saturated by using the previously described estimation strategy of inferring the temperature from an observable, Eq. (3.34). In this instance the observable is the energy of the system [JLM11], H, which may not be surprising because of how intertwined energy and temperature are as quantities within the realm of statistical mechanics[8].

Analogous to a GHZ state or NOON state being the optimal probe for phase estimation, Eq. (3.77) can be maximized to find the optimal probe for thermometry. The solution is an effective two level system with a single eigenstate having an energy of ϵ_- and $N-1$ eigenstates having a degenerate energy of ϵ_+, the relative error of such a probe is $\Delta^2\hat{T}/T^2 = \mathcal{O}(1/\log N)$ [Cor+15; MSC19]. Note that the information presented in this example holds only for fully thermalized systems, which may be a time consuming process. The analysis is significantly more complex for partially thermalized systems [Cor+15].

[8] On a macroscopic scale, temperature is an average quantity of a system composed of many many particles. This definition is somewhat ambiguous on a microscopic scale. In Eq. (3.75), temperature can be interpreted as a variable which governs the probability of the quantum system occupying a specific energy eigenstate.

4
Graph States as a Resource for Quantum Metrology

It is obviously very desirable to have an easy to implement quantum resource with a large span of applications. One class of quantum states which satisfies these criteria are graph states: a versatile resource for quantum computation and quantum communication. In this chapter, to help determine the full extent of the applicability of qubit graph states, we explore their practicality for the quantum metrology problem of phase estimation. Before beginning this work, it had been shown that cluster states (a subset of graph states) are an efficient resource for certain quantum metrology problems, namely with a non-local parameter encoding scheme [RJ09] or after undergoing local rotations [Fri+17]. We consider the standard (local) phase estimation problem and are able to quantify the effectiveness of a general graph state based on the shape of the corresponding graph [SM20]. Since our work has been published, others have explored the practicality of continuous variable graph states for quantum metrology [WF20].

4.1 Graph States

Graph theory [Wes+01] is a rich and diverse branch of mathematics. A *graph* is a structure used to model pairwise relationships with respect to a set of elements. A graph is devised of two types of elements: i) a set of *vertices* (or nodes) which are connected with ii) *edges*[1]. Graphs are a customary tool in mathematics - they

[1]This is the simplest description of a graph. More general graphs can have edges with assigned weights and/or a direction. These extra parameters are unnecessary for the scope of our work.

are the standard representation of the popular travelling salesmen problem and minimum colouring problem, for example. Outside of mathematics, graph theory is a tool to model all sorts of relations. In computer science, it can model the flow of information, where vertices are websites and an edge a hyperlink from one website to another. In animal biology, a vertex could signify a geographical region and the edges denote migration patterns for a species. With the broad scope of utility and existing research surrounding graph theory, it is unsurprising that it is used in the field of quantum information [HEB04].

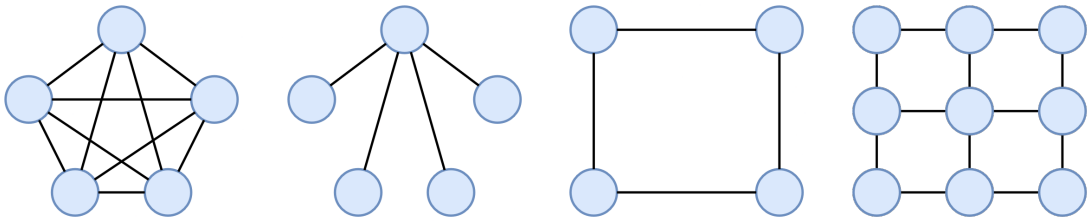
Graph states are an incredible useful resource in quantum information [Hei+06]. In the language of graph theory, quantum systems (qubits, qudits, CV states) are the vertices and entangling operations are the edges. These quantum states have a wide range of applications, including, but not limited to, cryptography [MS08; Qia+12], verification [MK20], quantum networks [PWD18; MMG19; HPE19], t-designs [Mez+18] and error correction [SW01]. Marginally more complex graphs, where the vertices are either a quantum system, a quantum operation or a quantum measurement, is the foundation of measurement based quantum computing [RB01; RBB03; Van+06]. In terms of implementation, graph states have been experimentally constructed using trapped ions [Bar+11; Lan+13], superconducting circuits [Son+17; Gon+19], squeezed states of light [Yok+13; CMP14] and photons [Lu+07; Gu+19; RBE19].

4.1.1 Graphical Representation

Formally, a graph is a set of vertices $V = \{v_1, \ldots, v_n\}$ and edges $E = \{e_1, \ldots, e_m\}$, where each edge $e_j = (v_{j_1}, v_{j_2})$ is a length-2 tuple of two vertices. The graph is denoted by $G = (V, E)$. In quantum information, the set of vertices correspond to quantum systems (for this work these are qubits) and the edges correspond to an entangling operation. Each qubit is prepared in the $|+\rangle$ state, and a controlled-Z operation is performed on the ith and jth qubit if $(v_i, v_j) \in E$. As an example, consider a 3 qubit star graph state, Fig. (4.1b), where the first qubit is the central qubit. The bra-ket representation of this quantum state is

$$\begin{aligned} |G\rangle &= CZ_{(1,2)}CZ_{(1,3)} \,|+++\rangle \\ &= \frac{1}{\sqrt{8}}\big(\,|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle - |101\rangle - |110\rangle + |111\rangle\,\big). \end{aligned} \tag{4.1}$$

Other graphical nomenclature used is this chapter is 'neighbourhood' and 'isolated vertex'. The neighbourhood of a vertex v, denoted as $N(v)$, is the set of



(a) Complete graph. (b) Star graph. (c) Cyclic graph. (d) Lattice graph.

Figure 4.1: Graphical representation of frequently used graphs in quantum information. (a) A complete graph (or fully connected graph) is where each vertex is connected to every other vertex; $E_a = \{(v_i, v_j)\ \forall v_i, v_j \in V_a\}$. (b) A star graph is where there is a central vertex which forms an edge with all of the other vertices; $E_b = \{(v_1, v_j)\ \forall j \geq 2\}$. (c) A cyclic graph is where the vertices are connected by a ring like series of edges; $E_c = \{(v_j, v_{j+1})\}$. (d) A lattice graph is where the vertices are arranged in an array. By using only single qubit Clifford operations, the complete graph state (a) and star graph state (b) can be transformed into the (all important) GHZ state using local Clifford operations. A cyclic graph (c) is one of the simplest models for a chain of quantum repeaters [AK17]. A lattice graph state (d) wrapped around itself to form a torus is the basic structure of topological quantum error correcting codes [BM06; BM07]. All four graphs could be used to represent a quantum network with varying complexities and purposes.

vertices which are connected to v: $N(v) = \{u \in V |\ (u, v) \in E\}$. A vertex w is said to be isolated if it has an empty neighbourhood: $|N(w)| = 0$.

4.1.2 Stabilizer Representation

Graph states belong to a larger family of quantum states called *stabilizer states*. The (general) stabilizer formalism does not have a graphical and illustrative analogue, instead, it is built upon mathematical symmetries and elegance. Stabilizer formalism, originally developed for quantum error correction [Got97] and adapted for measurement based quantum computing [RB01], is efficiently simulated [AG04] and verifiable [PLM18; MK20] due to the fact that the underlying structure is symmetries arising from the Pauli group. The set of stabilizer states is closed under local Clifford operations, and a large number of stabilizer states are highly entangled.

A quantum state $|\psi\rangle$ is said to be stabilized by an operator S if $S|\psi\rangle = |\psi\rangle$. An n qubit quantum state $|\psi\rangle$ is a stabilizer state if it is stabilized by n non-identity stabilizing operators $g_1, \ldots, g_n$ which i) all commute, ii) are multiplicatively independent and iii) are elements of the Pauli group $\pm\mathcal{P}_n$ [GMC17]. The bra-ket

representation of a stabilizer state is

$$|\psi\rangle\langle\psi| = \frac{1}{2^n}\prod_{j=1}^{n}\left(\mathbb{I} + g_j\right) = \frac{1}{2^n}\sum_{S\in\mathcal{S}} S, \tag{4.2}$$

where $\mathcal{S}$ is the stabilizer group of $|\psi\rangle$. Each $S \in \mathcal{S}$ stabilises $|\psi\rangle$ and is multiplicatively generated by $g_1, \ldots, g_n$ (hence the name generators). The generators are not necessarily unique, but the corresponding stabilizer group is unique. For example, the stabilizer group of the 3 qubit GHZ state, Eq. (2.7), can be written as $\langle X_1X_2X_3, Z_1Z_2, Z_2Z_3\rangle$ or as $\langle X_1X_2X_3, -Y_1Y_2X_3, -X_1Y_2Y_3\rangle$ (here the subscripts indicates which qubit a Pauli operator is acting on.

It is easy to verify that for all $1 \leq j \leq n$, operators of the form

$$g_j = X_j \bigotimes_{k\in N(j)} Z_k, \tag{4.3}$$

stabilize a graph state with neighbourhoods $N(1), \ldots, N(n)$. This follows from

$$X_j CZ_{(l,m)} X_j = \begin{cases} Z_l CZ_{(l,m)} & \text{if } j = m \\ Z_m CZ_{(l,m)} & \text{if } j = l \\ CZ_{(l,m)} & \text{otherwise} \end{cases}, \tag{4.4}$$

thus

$$\begin{aligned} X_j \bigotimes_{k\in N(j)} Z_k \,|G\rangle &= \Big(\bigotimes_{k\in N(j)} Z_k\Big)\Big(\prod_{(l,m)\in E} X_j CZ_{(l,m)} X_j\Big) X_j \,|+\rangle^{\otimes n} \\ &= \Big(\bigotimes_{k\in N(j)} Z_k\Big)^2 \Big(\prod_{(l,m)\in E} CZ_{(l,m)}\Big) \,|+\rangle^{\otimes n} \\ &= |G\rangle\,. \end{aligned} \tag{4.5}$$

The operators of the form Eq. (4.3) all commute and are multiplicatively independent, and hence correspond to the stabilizer group for a graph state. The stabilizer representation of the graph state from Eq. (4.1) is

$$|\psi\rangle\langle\psi| = \frac{1}{8}\left(\mathbb{I} + X_1Z_2Z_3\right)\left(\mathbb{I} + Z_1X_2\right)\left(\mathbb{I} + Z_1X_3\right). \tag{4.6}$$

In fact, every stabilizer state can be transformed to a (not necessarily unique) graph state [Sch01] by constructing a locally acting Clifford operator $C \in \mathcal{C}_1^{\otimes n}$ which maps

the generators for a stabilizer state to generators of the form in Eq. (4.3).

Because all non-identity Pauli operators have a trace of zero, it follows that for any Pauli operator Q and stabilizer state $|\psi\rangle$ with stabilizer group $\mathcal{S}$

$$\langle\psi|Q|\psi\rangle = \begin{cases} 1 & \text{if } Q \in \mathcal{S} \\ -1 & \text{if } -Q \in \mathcal{S} \\ 0 & \text{otherwise} \end{cases}. \tag{4.7}$$

4.2 Graph States For Phase Estimation

In order to gauge the practicality of graph states for quantum metrology, we restrict the problem to phase estimation. As discussed in **Chapter 3**, phase estimation is versatile in its applications and the expression for the QFI is much more manageable than the general expression. Having said that, it is still not obvious which quantum states achieve a quantum advantage when it comes to phase estimation. Of course, for qubit systems, entanglement is a required resource to surpass the SQL. However, entanglement does not guarantee Heisenberg-like scaling; it was shown in [Osz+16] that, on average, a randomly selected entangled quantum state would not attain a quantum advantage (even with the allowance of local unitary transformations). Notably though, it was shown in the same study that most symmetric states[2] are (up to local unitary transformations) an efficient resource for phase estimation. It is no surprise that the standard resources for phase estimation are highly symmetric, eg. the GHZ state [GLM04; GLM06], half-Dicke state [TA14] and spin squeezed states [Gro12; ZD14]. A sensible conclusion is that entanglement paired with symmetry makes for an efficient resource for phase estimation.

The canonical phase estimation problem encodes an unknown phase θ through a unitary of the form

$$U_\theta = e^{-i\theta\sum_{j=1}^{n} H_i} = \left(e^{-i\theta H}\right)^{\otimes n}, \tag{4.8}$$

where $H_j = H\ \forall j$ are locally acting Hermitian operators. In [SM20], we set $H = \frac{1}{2}X$, as this choice leads to an easily described class of states which approximately saturate the HL. That being said, the solutions and results can be generalized to any Hermitian generator by rotating beneficial graph states appropriately. Using

[2] Symmetric states, sometimes called permutation invariant states, are a class of quantum states which remain unchanged when any number of subsystems are swapped with one another.

Eq. (3.42), the QFI of an n qubit graph state $|G\rangle$ is

$$\mathcal{Q}(G) = \sum_{i,j=1}^{n} \Big(\langle G|X_i X_j|G\rangle - \langle G|X_i|G\rangle\langle G|X_j|G\rangle \Big). \tag{4.9}$$

This equation can be evaluated using the trace property of stabilizer states, Eq. (4.7), and the stabilizer group of graph states. For a graph without any isolated vertices $\langle G|X_i|G\rangle = 0$ for all j. The quantity $X_i X_j$ stabilizes $|G\rangle$ if and only if the neighbourhood of the ith qubit is equal to the neighbourhood of the jth qubit. By construction, the negation, $-X_i X_j$, never stabilizes $|G\rangle$. Therefore, the QFI of a graph state $|G\rangle$ with no isolated vertices is equal to the number of ordered pairs (i, j) such that $N(i) = N(j)$. For the sake of a mathematical expression

$$\mathcal{Q}(G) = \sum_{i,j=1}^{n} \delta_{N(i),N(j)}, \tag{4.10}$$

where $\delta_{x,y}$ is the Kronecker delta which evaluates to 1 if $x = y$ and 0 otherwise. One can conclude that the graph states, although not totally symmetric states, still require a form of internal symmetry (i.e pairs of qubits with equal neighbourhoods) to attain a quantum advantage.

As an example, all of the external vertices of a n qubit star graph state, Fig. (4.1b), have the same neighbourhood (the central vertex). Thus, the QFI is $\mathcal{Q}(G_{\text{star}}) = (n-1)^2 + 1$, which is approximately equal to the HL. This is unsurprising as it is a highly symmetric state. Conversely, an n qubit cyclic graph state, Fig. (4.1c), may appear to be highly symmetric at a graphical level (rotational symmetry), it does not have any permutation symmetries. An n qubit lattice graph state, Fig. (4.1d), similarly does not have any permutations and also is limited by the SQL. This is in accordance with [Fri+17], where it is stated that unmodified cluster states are not good resources for quantum metrology. Note that this does not contradict the results of [RJ09], where an unconventional parameter encoding scheme is used.

Because of the choice of $H_i = \frac{1}{2}X_i$, many highly symmetric states do not achieve a quantum advantage. For example, the complete graph, Fig. (4.1a), is invariant under any permutation and achieves the SQL. However, using the alternative choice for the unitary encoding $H_i = \frac{1}{2}Y_i$, the the QFI of the complete graph is the HL and the QFI of the star graph is the SQL. This alternative choice Hamiltonian also leads to an alternative, but more complicated, topological expression: the QFI is equal to the number of ordered pairs (i, j) such that $N(i) \cup \{i\} = N(j) \cup \{j\}$. The problem concerning the choice of the encoding Hamiltonian vanishes by allowing

for local transformations before the parameter is encoded. With this assumption, a graph state (or more generally, a stabilizer state) $|\psi\rangle$ is a practical resource for phase estimation if there exists a $C \in \mathcal{C}_1^{\otimes n}$ such that $C|\psi\rangle$ is a graph state whose corresponding graph has many pairs of vertices with identical neighbourhoods. Logically, the final possibility to examine is when the encoding Hamiltonian is set to $H_i = \frac{1}{2}Z_i$. However a quick computation leads to the conclusion that this choise leads to a QFI equal to the SQL of $\mathcal{Q} = n$ for any graph state.

4.2.1 Generalization To Stabilizer States

The QFI of a graph state was computed by finding the overlap of the Pauli operators of $\pm X_i$ and $\pm X_i X_j$ with the stabilizer group. This argument is not unique to graph states and can be made for any stabilizer state, further it can be reverse engineered to determine the number of stabilizer states which achieve a desired level of QFI.

Begin by defining the sets

$$A = \{X_1X_2, X_1X_3, \ldots, X_1X_n\}, \tag{4.11}$$

and

$$B_k = \{Q_1 \ldots Q_k | Q_j \in \{Y, Z\}\ \forall 1 \leq j \leq k\}, \tag{4.12}$$

where $k > 1$. The set A is ordered such that if a group is generated with the first $k-1$ elements, it will contain all operators of the form X_iX_j with $1 \leq i, j \leq k$ (and $i \neq j$). Each $b \in B_k$ will commute with all elements of said group. We do not allow $Q_j = \mathbb{I}$ as then there exists a $b \in B_k$ which anti-commutes with certain operators.

Next construct the stabilizer group

$$\mathcal{S} = \langle a_1, \ldots a_{k-1}, b, bg_1, \ldots, bg_{n-k}\rangle, \tag{4.13}$$

where $a_1, \ldots, a_{k-1}$ are all unique operators from the set A, $b \in B_k$ and $g_1, \ldots, g_{n-k}$ act exclusively on the final $n-k$ qubits of the quantum state and are the generators for an $n-k$ qubit stabilizer state. By construction, $\mathcal{S}$ does not contain any stabilizer of the form $\pm X_i$ or $-X_iX_j$. Therefore, similar to a graph state with no isolated vertices, the QFI is equal to the number of stabilizers of the form X_iX_j, which is k^2 by construction. To determine a bound on the number of stabilizers states which achieve a QFI of $n^{2-\varepsilon}$, labelled via $\tilde{N}(n;\varepsilon)$, we count the total number of possible stabilizer groups which is of the form of Eq. (4.13) with $k \geq n^{1-\varepsilon/2}$. Mathematically,

one obtains

$$\tilde{N}(n;\varepsilon) \geq \sum_{k \geq n^{1-\varepsilon/2}} \binom{n-1}{k-1} 2^k s_{n-k}, \tag{4.14}$$

where s_m is the number of m qubit stabilizer states [AG04]

$$s_m = 2^m \prod_{j=0}^{m-1} (2^{n-j} + 1). \tag{4.15}$$

It is quite apparent that $\tilde{N}(n;\varepsilon) \ll s_n$ for small ε. This is because of a few different factors. The first is that most quantum states do not saturate the HL [Osz+16]. The second is that the bound in question is restricted to the problem of phase estimation via the specific unitary encoding with $H_i = \frac{1}{2}X_i$. Third, to simplify the mathematics, it was demanded that operators of the form $\pm X_j$ or $-X_jX_k$ were not in the stabilizer group; discrediting some stabilizer states which would still achieve the necessary QFI. In retrospect, a tighter bound could have been achieved by allowing for other encoding operations and a more concrete mathematical analysis.

4.3 Bundled Graph States

As it was formerly mentioned, graph states are a resource with many applications. It would be very desirable and convenient if a specific graph state with a specific application was also a practical resource for quantum metrology. Evidently from Eq. (4.10) and the previously mentioned examples, most graph states are not a good resource for quantum metrology, at least not before undergoing some sort of transformation [Fri+17]. In order to capitalize on graph states which are multi-purpose, we provide a recipe to transform any graph into a (larger) graph which is practical for quantum metrology. The new graph maintains the underlying structure of the old graph and can still be used for the original purpose.

We name the new constructed graph a *bundled graph state*, as the construction process involves replacing individual qubits by a bundle of qubits with identical neighbourhoods in order to maximize the QFI.

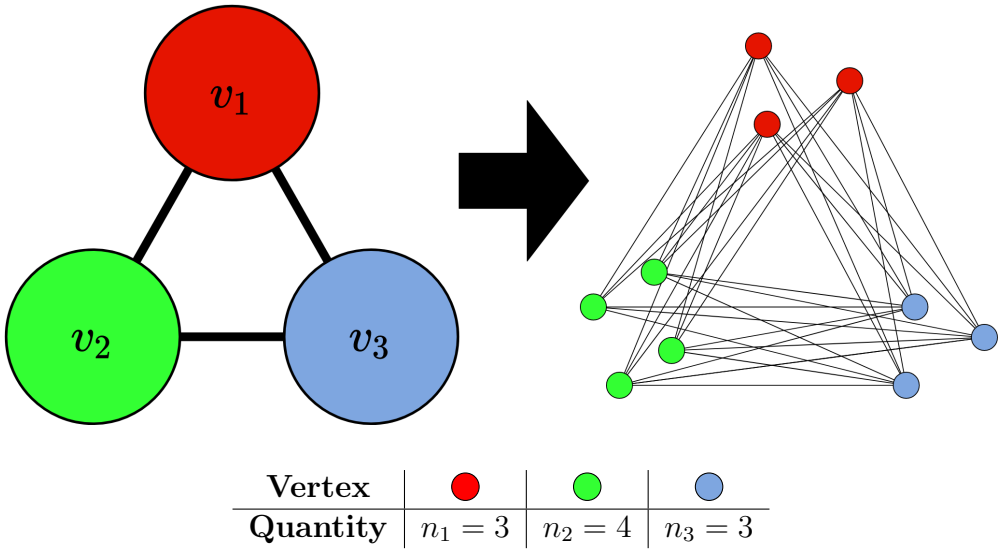


Figure 4.2: Transforming a $k = 3$ vertex graph into a $n = 10$ vertex bundled graph. The QFI of the corresponding bundled graph state (in this specific example) is $\mathcal{Q} = n_1^2 + n_2^2 + n_3^2 \approx n^{1.5}$.

4.3.1 Construction

The recipe transforms a smaller graph $G = (V, E)$ with k vertices (none of which are isolated) into a larger graph $G_{\text{bundled}} = (V', E')$ with $n \geq k$ vertices.

1. Begin with any k qubit graph state $G = (V, E)$ with no isolated vertices.
2. Vertex v_i is replaced with n_i vertices, labelled $v_i^{(1)}, \ldots, v_i^{(n_i)}$, with $\sum_{i=1}^{k} n_i = n$.
3. If $(v_i, v_j) \in E$ then $(v_i^{(a)}, v_j^{(b)}) \in E'$ $\forall a, b$.

The resulting graph $G_{\text{bundled}} = (V', E')$ has vertices

$$V' = \{v_1^{(1)}, \ldots, v_1^{(n_1)}, \ldots, v_k^{(1)}, \ldots, v_k^{(n_k)}\} \tag{4.16}$$

and edges

$$E' = \{(v_i^{(a)}, v_j^{(b)}) \; \forall a, b \mid (v_i, v_j) \in E\}. \tag{4.17}$$

The constructed bundled graph has many vertices with identical neighbourhoods: $N(v_i^{(a)}) = N(v_i^{(b)})$ $\forall i, a, b$. The above recipe is depicted in Fig. (4.2), in which an $n = 10$ vertex bundled graph from a smaller $k = 3$ vertex graph.

The QFI of a bundled graph state satisfies

$$\mathcal{Q}(G_{\text{bundled}}) \geq \sum_{i=1}^{k} n_i^2 \geq \frac{n^2}{k} = n^{2-\log_n k}. \tag{4.18}$$

If $k \ll n$, the resulting bundled graph approximately saturates the HL and the underlying structure of the graph state is preserved. Needless to say, the QFI is still dependent on the shape of the original graph. For example, a bundled cyclic graph state, where each of the k bundles contains an equal number of n/k qubits has a QFI

$$\mathcal{Q}(G_{\text{cyclic,bundled}}) = \frac{n^2}{k}. \tag{4.19}$$

A bundled star graph, built in the same manner, has a QFI

$$\mathcal{Q}(G_{\text{star,bundled}}) = n^2\big(1 - \frac{1}{k}\big)^2 + \frac{n^2}{k}. \tag{4.20}$$

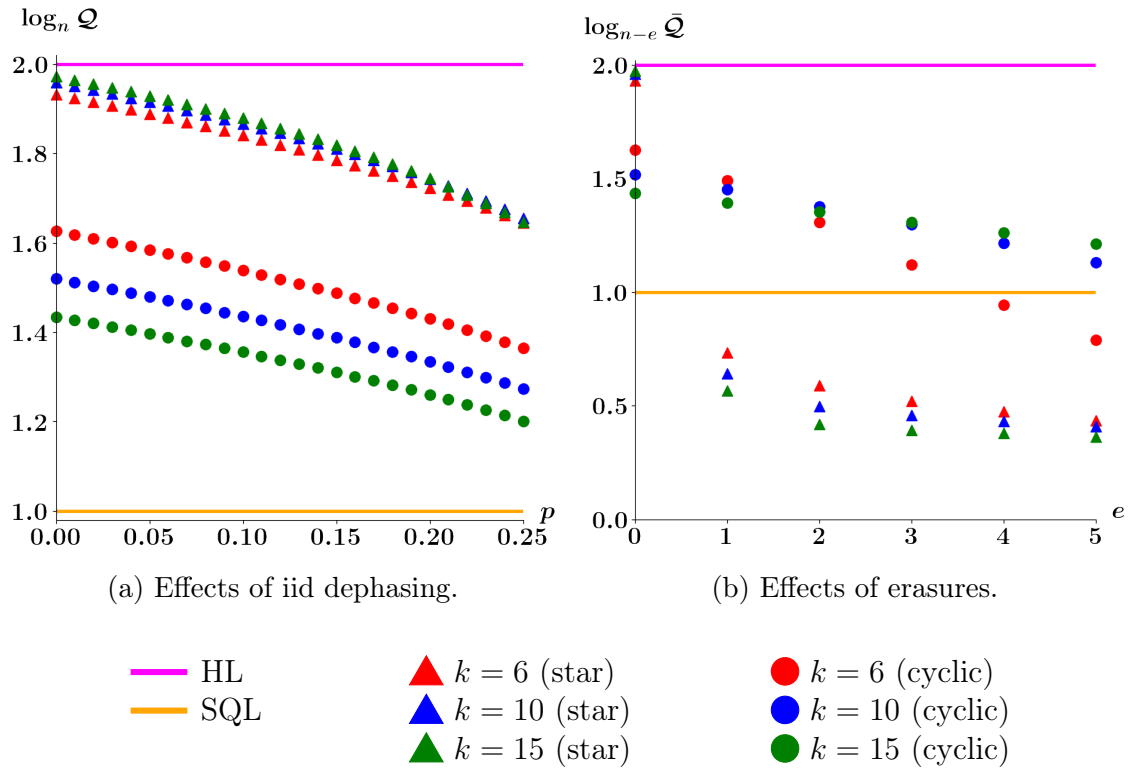
Unsurprisingly, $\mathcal{Q}(G_{\text{star,bundled}}) \geq \mathcal{Q}(G_{\text{cyclic,bundled}})$, this is due to the fact that the underlying structure of the star graph state contained symmetries, whereas the cyclic graph state did not. Nevertheless, both the bundled star graph state and the bundled cyclic graph state have a Heisenberg-like QFI.

4.4 Robustness

An important criteria for quantum states to possess to be a practical resource for quantum metrology is robustness against noise. Environmental noise is the primary obstacle for current quantum metrology technologies [EdMD11b; DKG12; Tsa13]. This topic, along with error correction based noise mitigation strategies is explored in much more detail in **Chapter 5**. In this chapter, a different approach to noise is taken: which is pinpointing resources which have a naturally built-in robustness. Two noise models are explored: i) iid dephasing, and ii) a finite number of erasures. These two noise models are frequently used in other noisy phase estimation problems [DKG12; KD13]. In particular, the GHZ state is famously fragile against the effects of loss and becomes useless for quantum metrology in a lossy environment [KD13]. We subject the graph states to the noise models to having the unknown parameter θ encoded. The QFI calculations for noisy graph states can be found in **Appendix A**.

As expected, the shape of a graph greatly influences the severity of the noise on the corresponding graph state. Without loss of generality, we again only consider

graphs which have no isolated vertices. To bound the QFI as elegantly as possible, we partition the vertices of a graph $G = (V, E)$ into disjoint subsets $U_1, U_2, \ldots, U_l, \ldots$ such that $\bigcup_l U_l = V$. The vertices are partitioned in accordance to commonly shared neighbourhoods, hence, if $v_i \in U_a$ and $v_j \in U_b$, then $N(v_i) = N(v_j)$ if $a = b$ and $N(v_i) \neq N(v_j)$ if $a \neq b$. We write that $|U_l| = u_l$ and the shared neighbourhood of U_l is M_l with $|M_l| = m_l$.



(a) Effects of iid dephasing.

(b) Effects of erasures.

Figure 4.3: Robustness of an $n = 120$ qubit bundled star graph states and bundled cyclic graph states subjected to (a) iid dephasing and (b) $e \leq 5$ erasures. In both scenarios, the bundled graphs have k equal size bundles of n/k qubits. After being subjected to iid dephasing (a), $\log_n \mathcal{Q}$ decreases linearly for small p. This is expected from Eq. (4.23), and ultimately, a quantum advantage is maintained. To gauge the effects of erasures (b), the quantity $\log_{n-e} \mathcal{Q}$ is plotted, where $\bar{\mathcal{Q}}$ is the average QFI of the bundled graph state after e erasures - it is necessary to take the average prior to the logarithm to avoid the problem of $\log_n 0$. Because bundled star graph states have an enormous amount of symmetry, a single erasure (regardless of where it occurs) will cause the QFI to fall below the SQL. In contrast, the bundled cyclic graph are more resilient to noise and can maintain an advantage after a small number of erasures; furthermore, the amount of qubits which are (on average) affected by the erasures decrease as k increases.

4.4.1 IID Dephasing

After being subjected to iid dephasing, each qubit has probability p of being dephased with respect to the Z operator. Define $Z_{\vec{j}}$ to be the Pauli operator which applies Z to all qubits indexed in $\vec{j}$ with $|\vec{j}| = j$. Post iid dephasing, an n qubit graph state $|G\rangle$ is mapped to

$$|G\rangle \to \sum_{\vec{j}} p^j (1-p)^{n-j} Z_{\vec{j}} |G\rangle\langle G| Z_{\vec{j}}, \tag{4.21}$$

which has a QFI of

$$\begin{aligned} \mathcal{Q}(G^{\text{dephasing}}) &\geq \sum_l \left((1-2p)^2 u_l^2 + 4p(1-p)u_l\right)\left(1-(2p(1-p)+1/2)^{m_l}\right) \\ &\geq (1-2p)^2\left(1-(2p(1-p)+1/2)^m\right)\mathcal{Q}(G), \end{aligned} \tag{4.22}$$

where $m = \min_l m_l$. The quantity $(2p(1-p)+1/2)^m$ is approximately zero for large enough m and small enough[3] p, using this approximation in tandem with the QFI of a bundled graph state Eq. (4.18),

$$\mathcal{Q}(G^{\text{dephasing}}_{\text{bundled}}) \geq (1-2p)^2 \frac{n^2}{k} = n^{2-\log_n k - \frac{4}{n}p + \mathcal{O}(p^2)}. \tag{4.23}$$

Therefore, for small p, bundled graph states retain a quantum advantage for phase estimation. This is shown in Fig. (4.3a), where the QFI of bundled star graph states and bundled cyclic graph states surpass the SQL for $p \leq 0.25$.

4.4.2 Erasures

A qubit becomes unusable after undergoing erasure, to model this the erased qubits are traced out

$$|G\rangle \to \text{Tr}_{\vec{e}} |G\rangle\langle G|, \tag{4.24}$$

where $\vec{e}$ indexes which qubits are erased. This maps the above state into an equally weighted mixed state[4]

$$2^{-|L_{\vec{e}}|} \sum_{\vec{j} \subseteq L_{\vec{e}}} Z_{\vec{j}} |G\rangle\langle G| Z_{\vec{j}}, \tag{4.25}$$

[3] $(2p(1-p)+1/2)^m < 0.006$ for $m \geq 10$ and $p \leq 0.05$.

[4] The mixed state in Eq. (4.25) is left as an n qubit state for clarity. The traced out systems are equivalent to maximally mixed states, $\mathbb{I}/2$, which are irrelevant with respect to the QFI.

where $L_{\vec{e}}$ is the set of vertices corresponding to the traced out qubits as well as their neighbourhoods and the sum is taken over all possible subsets of $L_{\vec{e}}$, denoted with $\vec{j} \subseteq L_{\vec{e}}$. As a consequence, the QFI is extremely dependent on the shape of the graph. In general

$$\mathcal{Q}(G^{\text{erasures } \vec{e}}) = \sum_l h_l(\vec{e}), \tag{4.26}$$

where

$$h_l(\vec{e}) = \begin{cases} u_l^2 & \text{if } M_l \nsubseteq L_{\vec{e}} \text{ and } U_l \nsubseteq L_{\vec{e}} \\ u_l & \text{if } M_l \nsubseteq L_{\vec{e}} \text{ and } U_l \subseteq L_{\vec{e}} \\ 0 & \text{otherwise} \end{cases}. \tag{4.27}$$

An interpretation, is that the 'noise' produced by an erasure effects all the similar qubits and propagates to the shared neighbourhood. Therefore, bundled graphs which were constructed from graphs that did not originally possess much symmetry are more robust against erasures then bundled graphs constructed from graphs with preexisting symmetries. This is witnessed in Fig. (4.3b), in which bundled cyclic graphs of varying size maintain a quantum advantage up to $e = 3$ erasures, in contrast, the QFI of the analogous bundled star graphs is below the SQL after a single erasure.

A possible method to circumvent erasure errors is to construct graph states with two types of qubits. One type would be used for metrology but prone to noise (e.g. the spin of an electron), and the other type is more naturally robust to noise but not used for metrology (e.g. the spin of a neutron). By constructing a hybrid graph state one could reduce the propagation of noise caused by the erasure of a sensing qubit. Graphically, this transformation can be described as adding a 'naturally robust' vertex in the center of each edge. If the naturally robust qubits are immune to erasures, the size of $L_{\vec{e}}$ would reduce drastically resulting in a higher QFI (on average).

4.5 Saturating The QCRB

Another important criteria for a quantum state to have in order to qualify as a practical resource for quantum metrology is the existence of a simple measurement scheme to saturate the QCRB. For a graph state with no isolated vertices, $|G\rangle$, this can be executed by measuring in the basis of a stabilizer, S_M, which consists entirely of Y and Z operators. Observe that the expected value of the observable

(with respect to the phase encoded graph state) is

$$\begin{aligned}\langle S_M \rangle &= \langle G| U_\theta^\dagger S_M U_\theta |G\rangle \\ &= \langle G| (U_\theta^\dagger)^2 S_M |G\rangle \\ &= \langle G| (U_\theta^\dagger)^2 |G\rangle \\ &= \sum_{j=0}^{\infty} \frac{(i\theta)^j}{j!} \langle G| \Big(\sum_{i=1}^{n} X_i \Big)^j |G\rangle\end{aligned} \tag{4.28}$$

For a graph state with no isolated vertices, the second order term is proportional to the QFI. Because the expectation value of an observable is real valued, the sum of all odd terms must be zero. Hence the above simplifies to

$$\langle S_M \rangle = 1 - \frac{\theta^2}{2} \mathcal{Q}(G) + \mathcal{O}(\theta^4). \tag{4.29}$$

Using the error propagation formula, the variance of the estimate scales as

$$\frac{\Delta^2 S_M}{|\partial_\theta \langle S_M \rangle|^2} = \frac{\theta^2 Q(G) + \mathcal{O}(\theta^4)}{\theta^2 Q(G)^2 + \mathcal{O}(\theta^4)} = \frac{1}{\mathcal{Q}(G)} + \mathcal{O}(\theta^2) \approx \frac{1}{\mathcal{Q}(G)}. \tag{4.30}$$

The above approximation is only valid when the phase being estimated is very small, $\theta \approx 0$, fortunately this is naturally the regime explored for phase estimation. If the unknown phase is large, but it is known up to approximation because of a pre-existing model or another estimate, then the quantum state can be first transformed by local unitary operations such that the effective phase is small.

The condition that a graph state has a stabilizer S_M which only consists of Y and Z operators is necessary for $S_M U_\theta = U_\theta^\dagger S_M$. Such a stabilizer is not guaranteed to exist and depends on the shape of the graph. For example, it always exists for bundled star graph states[5], but for bundled star graph states, it exists only when $k = 0 \mod 4$[6]. If the graph state does not have such a stabilizer, a solution can be remedied using an ancillary qubit. Let S_M be the stabilizer with as many Y or Z operators, in any index which there is not Y or Z operator, entangle the corresponding qubit to the new ancillary qubit with a controlled-Z operation. This will form an $n+1$ qubit graph state where the stabilizer $g_{n+1} S_M$ consists of entirely of Y and Z operators, thus the new graph, which would have a very similar structure to the original graph, can approximately saturate the QCRB with a simple single

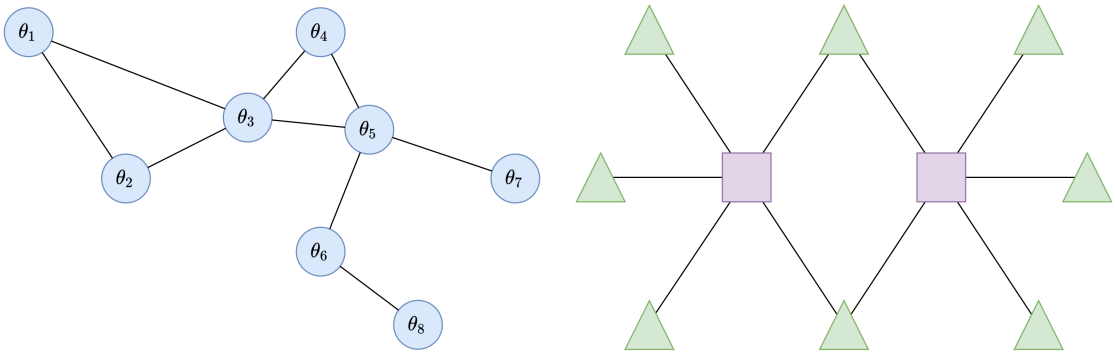
[5] Take the product of the generator of a central qubit and a generator of an external qubit.

[6] Divide the bundles into sequences of four. Take the product of a generator from the two central bundles from each group of four.

qubit measurement scheme.

4.6 Quantum Sensing Networks

An immediate application for graph states with respect to parameter estimation problems and metrology is quantum sensing networks [Kóm+14; Kóm+16; Eld+18; Ge+18; PKD18; ZZS18; Qia+19; Rub+20; Guo+20]. A quantum network is collection of nodes and edges, where the nodes have some quantum functionality and an edge represent some form of connection between a pair of nodes, this can be either entanglement of a quantum channel [Kim08; Van12; Sch+16; WEH18]. This is a much more general framework than the graph state framework, nonetheless the similarities between the two simplify the adaptation of a graph state into a quantum network [MMG19; HPE19]. A quantum sensing network is a quantum network designed for quantum parameter estimation. Quantum sensing networks come in two flavours depending on the functionality of the nodes and edges.



(a) Type 1 Quantum Sensing Network. (b) Type 2 Quantum Sensing Network.

Figure 4.4: There are two main descriptions for quantum sensing networks. The first type (a) of quantum sensing networks aligns with the description of a graph state, where a node represents a qubit and an edge represents an entangling operation. This type of quantum network is a popular framework for multiparameter quantum problems [PKD18; Rub+20], as each node can encode a different unknown parameter θ_j. The second type (b) of quantum sensing networks resembles the usual description of quantum networks [Van12], where an edge represents a quantum channel between two nodes. In particular, not all nodes are created equal and serve different purposes. In this schematic the central square nodes distribute quantum states to the exterior triangle nodes where an unknown parameter is encoded, the encoded quantum states are then returned to a central node to be measured.

The first type of quantum sensing networks is when the nodes represent a quantum state the edges represent a form of entanglement, depicted in Fig. (4.4a). Evidently, graph states are a subset of possible quantum sensing networks. Quantum sensing networks, with a suitable choice for entangling operations and initialized quantum states, have been shown to be an effective resource for multiparameter quantum metrology problems [PKD18; Rub+20]. Graph states are no exception, and thus a future natural direction for this work is to formally classify utility of graph states for quantum metrology in the multiparameter setting. Likely, the most efficient graphs will resemble bundled graph states where a different parameter is encoded into a different bundle.

The second type of quantum sensing networks is when the nodes have different technological functionality and edges represent a quantum channel, depicted in Fig. (4.4b). For example, the authors of [Kóm+14; Kóm+16] construct a quantum network where a central node is much more powerful technologically than the exterior nodes. There, the central node prepares quantum states, which are then distributed to exterior nodes where a local phase is encoded, after which the encoded quantum state is returned to the central node to be measured. A current project of mine is combining the results from this chapter and the cryptographic protocols outlined in **Chapter 6** to devise a notion of a secure quantum sensing network for phase estimation problems.

4.7 Discussion

To recapitulate, graph states are applicable to many disciplines of quantum information and can be implemented with different technologies. In our work [SM20], we showed that quantum metrology problems can be added to the versatility of graph states. This was done by constructing a class of graph states, called bundled graph states, which have a Heisenberg-like QFI with respect to phase estimation. By design, bundled graph states can have any desired underlying structure, making them multi purposeful.

In addition to the Heisenberg-like QFI, graph states are robust against iid dephasing and (conditional on the shape of the graph) a small number of erasures. As a comparison, the GHZ state is similarly robust against dephasing but cannot tolerate a single erasure [TA14]. Even though we explored specific error models, we expect similar robustness results in other settings. For example errors during or after the parameter encoding, or a spatially correlated noise model [JCH14], in

which vertices (or bundle of vertices) of a graph is subjected to different error rates.

Lastly, a simple measurement scheme is presented to approximately saturate the QCRB. Even though this can always be done in theory by measuring in the basis of the symmetric logarithmic derivative [BC94], doing so is unfeasible for real world quantum technologies. The measurement scheme we present uses local Pauli measurements, which is realizable for real world quantum technologies [Wal+12].

There are a number of exciting future perspectives for graph states and quantum metrology. One direction is to explore more general scenarios, such as metrology problems other than phase estimation or phase estimation with non-local parameter encoding unitaries [Lui04]. Another direction is to adapt the underlying structure of a graph state to that of a quantum sensing network [Kóm+14; Kóm+16; Eld+18; Ge+18; PKD18; ZZS18; Qia+19; Rub+20; Guo+20]. Likely, the most efficient graph states to adapt to a quantum sensing network problem is bundled graph states. This is because the inherent symmetries which boost their utility for quantum metrology remains unchanged in a multiparameter setting. Of course, this needs to be shown formally and may not be so straightforward to devise a measurement scheme with compatible measurements.

5
Limits of Error Correction for Quantum Metrology

Noise is the greatest obstacle for quantum metrology that limits the achievable precision and sensitivity [EdMD11a; EdMD11b; DKG12]. As a noisy system evolves in time, it becomes more and more difficult to distinguish the effects of the encoding Hamiltonian and the effects of noise [Haa+16]. A proposed solution to mitigate the effects of noise is to repeatedly perform quantum error correction [Kes+14; Dür+14; Arr+14; LYO15]. Recently, it has been shown that if the encoding Hamiltonian and the environmental noise satisfy an orthogonality condition, then the HL may be recovered indefinitely [DCS17; Zho+18]. This euphonic conclusion has the added caveat that the assumed frequency of which error correction is performed is infinite. Needless to say, this is an impractical assumption for current quantum technologies, where the rate of implementable error correction is on a similar time scale to the dephasing rates of spin qubits [Cra+16; Ofe+16] and superconducting qubits [Dut+07; Tam+14].

In this chapter, we determine the limitations of error correction enhanced quantum metrology by accounting for imperfections of near term quantum technologies. These include a non-infinitesimal wait time between applications of error correction, noisy ancillary qubits and imperfect error correction operations. The work done in [Kes+14] makes similar assumptions, however higher order error terms are ignored, which is equally presumptuous as infinitely frequent applications of error correction.

5.1 Environmental Noise And Errors

Quantum systems are extremely sensitive to small perturbations. These perturbations can arise from interactions with external degrees of freedom, e.g. an electron getting excited by an incident photon, or from the finite precision in which quantum operations and control can be performed. These interactions alter the evolution of a quantum system in an undesirable fashion, where the final quantum state is not the targeted quantum state in an idealistic scenario. This is perhaps the biggest hurdle in creating quantum technologies [SÁ16], to such an extent that many have come to accept the current inevitability of errors and search for problems which may be solved with noisy intermediate-scale quantum (NISQ) technologies [Pre18; TM20; Bha+21].

The standard nomenclature for 'interactions with external degrees of freedom' is environmental noise. Models for open quantum systems subject to environmental noise comes in many flavours [Gar91; BP+02; Cle+10] and ultimately depend on the type of quantum technology. Photonic systems are prone to lossy effects [WCW14], whereas spin systems are prone to decoherence effects [Zur06]. Similarly, the consequences of noise is model dependent, but in principle entanglement in composite systems is lost, and the likely reason why quantum effects are not observed at a macroscopic scale [Sch05; Zur06].

5.1.1 Noisy Quantum Metrology

In the past decade, the effects of noise on quantum metrology problems have been well established [EdMD11a; EdMD11b; DKG12; Cha+13; Tsa13; KD13; JCH14; Kol14; DJK15; Haa+16]. Optical systems are prone to loss and diffusion [Lee+09; Dem+09; KSD11; Zha+13; DJK15], while atomic systems are prone to dephasing and decoherence [SC07; BS13; MFD14; ZYL14]. In principle, as a noisy system evolves in time, it becomes more difficult to extract information about the encoded unknown parameter(s), and as a consequence of lost entanglement, the sensitivity is limited to that achievable by classical approaches [CHP12].

The canonical example of a noisy quantum metrology scheme involves n qubits governed by two interactions. The first is a signal ω which causes a detuning in each of the qubits, represented by $H = \frac{\hbar\omega}{2}\sum_{m=1}^{n} Z_m$. The second, an interaction with the environment which causes dephasing with rate γ in the X direction. Lastly, the qubit evolves in accordance to its natural resonance frequency, which is assumed to be known to a high degree of precision. In the rotating reference frame, where the

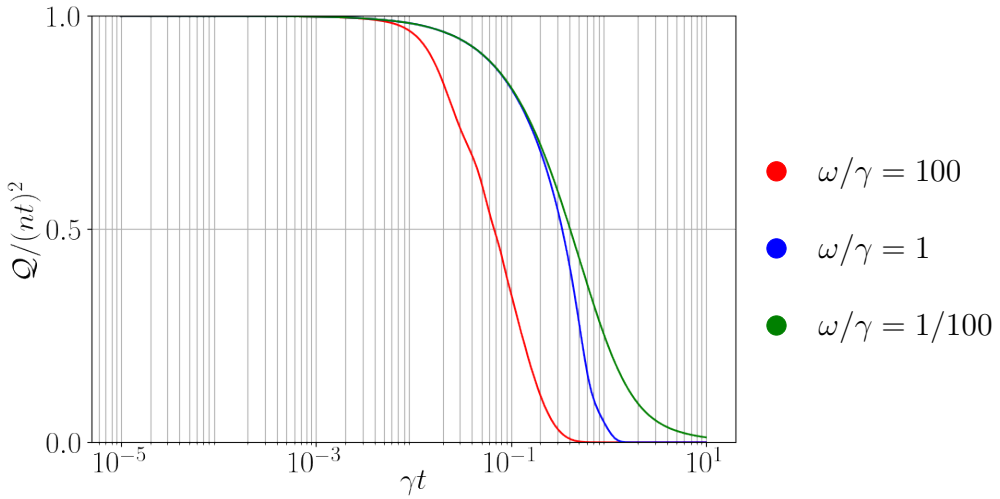


Figure 5.1: Normalized QFI $\mathcal{Q}/(nt)^2$ after an $n = 10$ qubit GHZ state is used for phase estimation in the presence of environmental decoherence, Eq. (5.1). Regardless of the signal-to-noise ratio, ω/γ, the QFI tends to zero around $2\gamma t \approx 1$.

natural frequency of the qubit is suppressed, the Lindbladian master equation can be written as [RH12]

$$\frac{d\rho}{dt} = -\frac{i}{\hbar}[H, \rho] + \gamma \sum_{m=1}^{n} (X_m \rho X_m - \rho). \tag{5.1}$$

After time t the QFI of the system can be computed (see **Appendix B**) to be

$$Q_{\text{noisy}} = n^2 t^2 \Big(1 - \big(2 - \frac{4}{3n}\big)\gamma t\Big) + \mathcal{O}(t^4). \tag{5.2}$$

In the short time limit, where the first two non-zero terms of the Taylor expansion dominate the behaviour of the QFI, the HL is lost once the quantity $2\gamma t$ becomes large. This is true regardless of the value of ω, as depicted in Fig. (5.1). This is not a practical time scale for quantum metrology [Hue+97], specifically in the interest of small values of ω where it is necessary for the system to evolve for a long enough time to distinguish between the effects of the signal and imperfections of real world measurement technologies.

There are a number of proposed strategies to mitigate the effects of noise. A passive approach is to engineer the noise model so that is better suited for quantum metrology. For example, non-Markovian noise models[1] can be tailored to outper-

[1] A Non-Markovian noise model is one which does not use the Born-Markov [Kol20] approximation to formulate the master equation.

form standard Markovian noise models [CHP12; Ber13]. Similarly, decoherence free subspaces (where qubit dephasing is not independent) outperform the standard uncorrelated depashing noise models [Dor12]. A more active approach is to monitor the effects of the environment using continuous measurements [Cle+10; PH16; Alb+18; Ros+20].

Quantum control is a very promising technique to suppress the effects of noise on quantum metrology [Sek+17]. Broadly speaking, the quantum system is occasionally modified, and if done appropriately can reduce the impact of noise. [Zhe+15] proposes feedback to based off of a coupled to a cavity or reservoir to 'reverse' the effects of noise. Dynamical decoupling protocols [Ron+11; SÁS12; SSD16] apply a sequence of unitary operation in rapid succession can cancel out the effects of noise. Signal amplification in optical systems can be used to mitigate the effects of loss [Cav81; Ou12; Fra+21]. This chapter focuses on incorporating quantum error correction as a means of control.

5.2 Quantum Error Correction

The fragility of quantum systems is a major obstacle for quantum computing [Unr95; RH96]. Suppose each quantum operation has a small probability of being done incorrectly: $\varepsilon \ll 1$; embedding an error in the quantum system. Then the probability that no errors occur after N operations is $(1-\varepsilon)^N$, which will decrease to zero as N increases. *Quantum error correction* [DMN13] is a vital tool developed to combat the effects of noise and actualize fault tolerant quantum computing [Pre98]. Using clever encoding schemes, in which quantum states are encoded into larger systems (often called 'logical' quantum states), the effects of environmental decoherence can be reduced substantially enough such that arbitrarily long protocols and computations can be fulfilled.

The *no-cloning theorem*[2] [WZ82] and the *collapse of the wave-function* are the predominant reasons as to why classical error correction techniques cannot be seamlessly integrated into a quantum framework. Furthermore, qubits are susceptible to bit flips and phase flips, for which there is no classical analogue for the latter. Despite the challenges and constraints, primitive error correction models and protocols were established in the 1990's [Sho95; Ste96a; Ste96b; CS96; Ben+96; Got96; Got97; Kit97]. In the last two and half decades, the field of quantum error correction has

[2] It is impossible to create an independent and identical copy of an arbitrary unknown quantum state.

flourished. Nowadays, a range of error correction protocols exist, such as topological codes [Kit97; BM06; BM07], permutation invariant codes [PR04; Ouy14; OSM19] and approximate codes [Leu+97; SW02]; each with their own advantages and disadvantages. In addition, quantum error correction has been experimentally demonstrated using different resources, such as spin qubits [Dut+07; Tam+14; Cra+16], continuous variable optical systems [Aok+09] and superconducting circuits [Ree+12; Ofe+16].

5.2.1 Example: Bit-Flip Code

A bit-flip error, denoted by $\mathcal{E}$, maps the quantum state $|0\rangle$ to the quantum state $|1\rangle$ and vice versa. If p is the probability of a bit-flip error, then

$$\mathcal{E}(\rho) = (1-p)\rho + pX\rho X. \tag{5.3}$$

The three qubit bit-flip code [Got97] is a rudimentary error correcting code designed to correct a single bit-flip error. The physical states $|0\rangle$ and $|1\rangle$ are encoded[3] into three qubit logical states $|0_L\rangle = |000\rangle$ and $|1_L\rangle = |111\rangle$ respectively, and in general,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \rightarrow |\psi_L\rangle = \alpha\,|0_L\rangle + \beta\,|1_L\rangle\,. \tag{5.4}$$

Each of the three qubits physical qubits are independently susceptible to a bit-flip error

$$\begin{aligned}
&\mathcal{E}(|\psi_L\rangle\langle\psi_L|) = \\
&(1-p)^3\,|\psi_L\rangle\langle\psi_L| \\
&+p(1-p)^2\big(X_1\,|\psi_L\rangle\langle\psi_L|\,X_1 + X_2\,|\psi_L\rangle\langle\psi_L|\,X_2 + X_3\,|\psi_L\rangle\langle\psi_L|\,X_3\big) \\
&+p^2(1-p)\big(X_1X_2\,|\psi_L\rangle\langle\psi_L|\,X_1X_2 + X_1X_3\,|\psi_L\rangle\langle\psi_L|\,X_1X_3 + X_2X_3\,|\psi_L\rangle\langle\psi_L|\,X_2X_3\big) \\
&+p^3X_1X_2X_3\,|\psi_L\rangle\langle\psi_L|\,X_1X_2X_3,
\end{aligned} \tag{5.5}$$

equivalently, there is a probability: $(1-p)^3$ of no errors occurring, $3p(1-p)^2$ of exactly one error occurring, $3p^2(1-p)$ of exactly two errors occurring, or p^3 of exactly three errors occurring. Assuming that p is small, it is far more likely that 0 or 1 errors occur than 2 or 3 errors occur. Thus, by comparing the parity of the three qubits (which can be done using non-destructive and entangled measurements), one

[3] The encoding can be implemented with two ancillary $|0\rangle$ states and controlled-X operations.

can apply a 'majority-is-correct' correction rule, and (with high probability) recover the quantum state[4]. Formally, this measurement is better known as a *syndrome measurement* or *syndrome diagnosis*, the measurement results are better known as *error syndromes* and the correction rule is better known as a *recovery operation*. The error syndromes and recovery operations of the bit-flip code are listed in Table (5.1).

Error Syndrome	Recovery Operation
$\|000\rangle\langle 000\| + \|111\rangle\langle 111\|$	$\mathbb{I}$
$\|100\rangle\langle 100\| + \|011\rangle\langle 011\|$	X_1
$\|010\rangle\langle 010\| + \|101\rangle\langle 101\|$	X_2
$\|001\rangle\langle 001\| + \|110\rangle\langle 110\|$	X_3

Table 5.1: The error syndromes and corresponding recovery operations for the bit-flip code.

The bit-flip code, is not 'technically' an error correction code, because, although it can correct bit-flip errors, it cannot correct any error, for example phase-flips. One can correct a single phase-flip using a similarly constructed phase-flip code [Got97]. Notably the 9-qubit code is constructed by superimposing the phase-flip and bit-flip code, which can correct any single qubit error [Sho95]. It was later shown that any single qubit error can be corrected using a more compact code of five qubits [Laf+96].

5.3 Error Correction Enhanced Quantum Metrology

It was shown in [Kes+14] that repeated applications of error correction can be used to significantly increase the sensitivity of a quantum probe for quantum metrology. Since then, the extent of error correction enhanced quantum metrology has been well explored[5]: the general limitations have been established [Dür+14; Arr+14; LYO15; DCS17; Zho+18; ZJ20], and codes have been engineered for specific scenarios [Her+15; MB17; LC18; Lay+19; ZPJ20; Wan+21]. Error correction enhanced

[4]The quantum state is recovered if zero or one errors occurred, but not if two or zero errors occurred. If $p \ll 1$, the former scenario is much more likely.

[5]As it happens, the converse setting of using mathematical techniques of quantum metrology for quantum error correction has also been explored in [KD21], where QFI bounds were used to provide a proof of the approximate Eastin-Knill Theorem.

magnetometry has been experimentally realized in [Und+16], where the sensing time exceeded the natural dephasing times of the spin qubits.

For general Markovian noise, quantum error correction can be used to correct errors which can be distinguished from the Hamiltonian which encodes the signal (transverse noise). When the signal Hamiltonian and environmental noise commute (parallel noise), error correction cannot be used. Parallel noise can be corrected for non-Markovian noise models [LC18; Lay+19] or using continuous measurements [Alb+18].

5.3.1 Theoretical Limitations: Recovering The HL

Recall from **Chapter 2** that the dynamics of a general Markovian noise model are governed by the master equation

$$\dot{\rho}(t) = -\frac{i}{\hbar}[H, \rho(t)] + \sum_{j=1}^{d^2-1} \gamma_j \big[L_k \rho(t) L_k^\dagger - \frac{1}{2}\big\{\rho(t), L_k L_k^\dagger\big\}\big], \tag{5.6}$$

$L_1, \ldots, L_{d^2-1}$ are Lindblad operators. It follows that, for a small time τ, the evolution can be written as

$$\rho(t+\tau) = \rho(t) - \frac{i}{\hbar}[H, \rho(t)]\tau + \sum_{j=1}^{d^2-1} \gamma_j \big[L_k \rho(t) L_k^\dagger - \frac{1}{2}\big\{\rho(t), L_k L_k^\dagger\big\}\big]\tau + \mathcal{O}(\tau^2). \tag{5.7}$$

It was shown in [DCS17; Zho+18] that for a general transverse noise model, an error correction code can be constructed, which when applied, will not interrupt the encoding Hamiltonian, i.e

$$\rho(t) - \frac{i}{\hbar}[H, \rho(t)]\tau \tag{5.8}$$

and correct first order errors, i.e

$$\sum_{j=1}^{d^2-1} \gamma_j \big[L_k \rho(t) L_k^\dagger - \frac{1}{2}\big\{\rho(t), L_k L_k^\dagger\big\}\big]\tau. \tag{5.9}$$

The distinguishable criteria (transverse noise) is called Hamiltonian-not-in-Linblad span in [Zho+18], because the necessity condition is rephrased as

$$H \notin \text{span}\{\mathbb{I}, L_j, L_j^\dagger, L_j^\dagger L_k\}, \tag{5.10}$$

where the span is taken over all subscripts j and k. It is demonstrated that, if the frequency at which error correction is performed is fast enough such that the higher order evolution terms are negligible, $\mathcal{O}(\tau^2) \to 0$, then the HL can be maintained indefinitely.

5.3.2 Practical Limitations: Current Quantum Technologies

Unfortunately, the mathematical assumption of arbitrarily fast error correction does not coincide with current quantum technologies. In fact, higher order error terms should not be ignored whatsoever, reason being that current error correction rates scale similarly to current dephasing rates [Dut+07; Sch+11; Tam+14; Cra+16; Ofe+16]. The experimental realization of error correction enhanced quantum metrology [Und+16] had a wait time between periods of error correction of 20μs (or 50kHz) - comparable to the reported decoherence rate of 30kHz. This experiment used a single NV center as a sensor and performed two applications of error correction.

Even supposing that the higher order terms $\mathcal{O}(\tau^2)$ in Eq.(5.7) are negligible compared to the first order approximation, the argument in itself falls short of expectations. If t is the sensing time, and τ is the time between applications of error correction; the assumption of τ being arbitrarily small is equivalent with the number of rounds of error correction, t/τ, being arbitrarily large. Although the higher order evolution term is negligible after a single round of error correction, which in turn adds a negligible amount of uncertainty to the final quantum state, this does not necessarily imply that the total uncertainty added to the quantum state after t/τ rounds is also negligible.

Furthermore, current quantum error correction technologies are not perfect. Ancillary qubits are also encumbered to the effects of noise. Syndrome diagnosis and recovery operations cannot be implemented with perfect fidelity. These imperfections will hinder the utility of the quantum state for quantum metrology.

5.4 Our Model

A more pragmatic approach for error correction enhanced quantum metrology is to make no assumptions regarding the time between applications of error correction and draw conclusions from an exact solution. It should be noted that the noise models in [DCS17; Zho+18] are completely general. Inevitably, obtaining an exact solution for an arbitrary noise model is infeasible, which is why we use a relevant

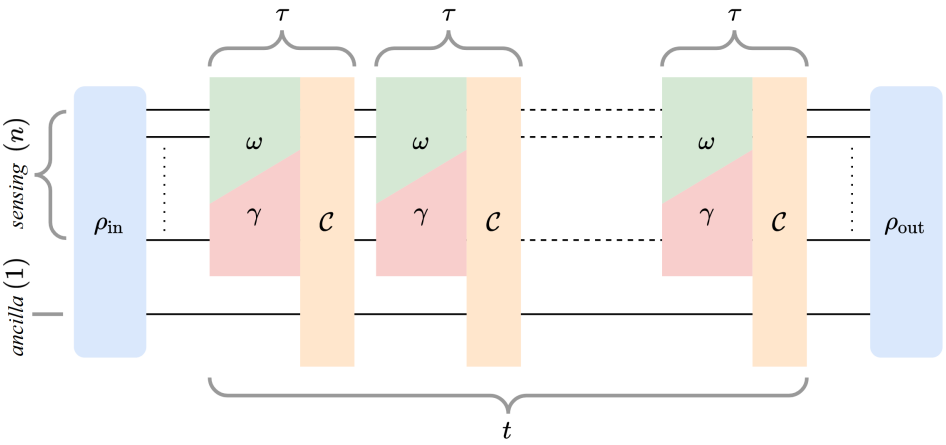


Figure 5.2: Schematic of our error correction enhanced quantum metrology model. The input state, ρ_{in}, is initialized as an $n+1$ qubit GHZ state composed of n sensing qubits and one ancillary qubit. The sensing qubits are influenced by a signal ω and dephasing γ. The parity check code, denoted by $\mathcal{C}$, is repeatedly applied after a given time τ to mitigate the effects of dephasing. The final quantum state used for parameter estimation, ρ_{out}, undergoes t/τ rounds of error correction. The scheme can easily be generalized; allowing for arbitrary input states, error correction strategies and more ancillary qubits.

noise model: dephasing in a direction orthogonal to the signal, see Eq. (5.1).

Similarly, we make use of a realizable error correction code: a parity check code [HBD09; FGV15; Rof+18]. A parity check code makes use of an ancillary qubit which is less sensitive to environmental interactions (and thus less noisy). For example, the experiment in [Und+16] used an electron spin for sensing and a nuclear spin as the ancillary qubit. In each application of error correction, the syndrome diagnosis outputs the parity between individual sensing qubits and the ancillary qubit. The subsequent recovery operation will correct any qubits which demonstrated a difference in parity by applying an X operation.

In our model, exhibited in Fig. (5.2), the quantum state is initialized as an $n+1$ qubit GHZ state, where n qubits are used for sensing and the remaining one qubit (which is more resistant to environmental noise) acts as an ancilla for error correction. The sensing qubits are influenced by a signal ω and dephasing with rate γ. The sensing qubits evolve per Eq. (5.1) for time τ, after which the parity check code is applied; the procedure is then repeated t/τ times where t is the total sensing. Without loss of generality, it is assumed that t/τ is an integer. The set-up is similar to that of [Kes+14], however the authors disregard higher order error terms, which is similarly presumptuous to assuming an arbitrarily small τ.

To augment the reality of our model, we account for other hindrances current error correction technologies are burdened by: noisy ancilla and imperfect syndrome diagnosis. The noisy ancilla is subjected to a dephasing rate ξ, which changes the master equation to

$$\frac{d\rho}{dt} = -\frac{i}{\hbar}[H,\rho] + \gamma\sum_{m=1}^{n}(X_m\rho X_m - \rho) + \xi(X_{n+1}\rho X_{n+1} - \rho), \tag{5.11}$$

where the ancillary qubit is indexed by the subscript $n+1$. Imperfect syndrome diagnosis is simulated by assuming that the syndrome diagnosis is incorrect with probability p, which results in an unnecessary recovery operation (or lack thereof).

5.5 Results

A completely general result for the final quantum state after t/τ rounds of error correction with a noisy ancilla and imperfect syndrome diagnosis is derived in **Appendix B**. The general solution is quite complicated and difficult to analyse. For clarity, each subcase is analysed individually: i) ideal error correction ($\xi = 0$, $p = 0$), ii) noisy ancilla ($\xi \neq 0$, $p = 0$), and iii) imperfect syndrome diagnosis ($\xi = 0$, $p \neq 0$).

5.5.1 Ideal Error Correction

In the ideal error correction scenario (noiseless ancilla and perfect error correction), after t/τ rounds of error correction, the final quantum state can be expressed as a bipartite mixed state

$$\rho = \frac{1+r^{nt/\tau}}{2}\left|\psi_+\right\rangle\!\left\langle\psi_+\right| + \frac{1-r^{nt/\tau}}{2}\left|\psi_-\right\rangle\!\left\langle\psi_-\right|, \tag{5.12}$$

where

$$\left|\psi_\pm\right\rangle = \frac{1}{\sqrt{2}}\big(\left|0\right\rangle^{\otimes n+1} \pm e^{in\phi t/\tau}\left|1\right\rangle^{\otimes n+1}\big), \tag{5.13}$$

and

$$re^{\pm i\phi} = e^{-\gamma\tau}\big(\cos(\Delta\tau) + \frac{\gamma \pm i\omega}{\Delta}\sin(\Delta\tau)\big), \tag{5.14}$$

with $\Delta = \sqrt{\omega^2 - \gamma^2}$. There is no mathematical issue when $\omega^2 < \gamma^2$, in this regime the trigonometric functions are replaced by the corresponding hyperbolic functions (as per their definition). Because the quantum state is evaluated immediately after

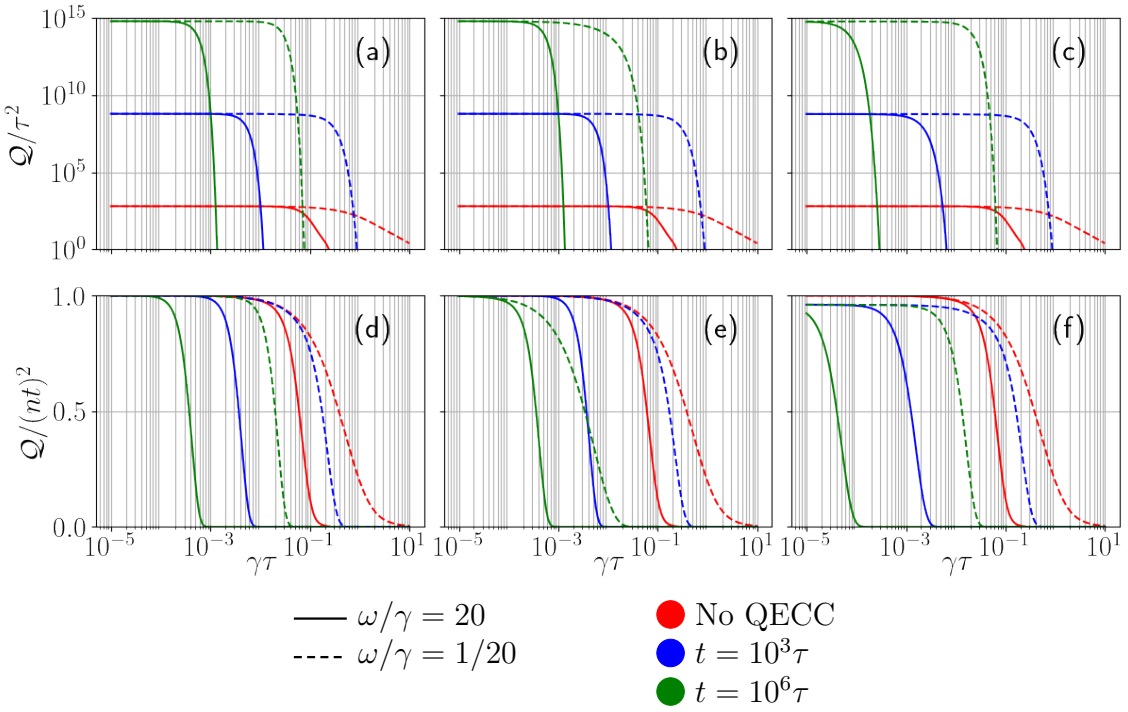


Figure 5.3: Plot of $\mathcal{Q}/\tau^2$ for an $n = 25$ qubit GHZ state after undergoing repeated error correction with (a) ideal error correction, (b) a noisy ancilla ($\xi/\gamma = 10^{-4}$), and (c) imperfect syndrome diagnosis ($p = 0.01$), with total sensing times $t/\tau = 10^3, 10^6$. The characteristics of a noisy state without the inclusion of a quantum error correction code (QECC) after sensing time $t = \tau$ is also displayed. As the total sensing time t increases, the necessary rate at which error correction is needed to maintain the HL increases. Hence the reason why the curve with $t = 10^6\tau$ begins to decrease before the curve with $t = 10^3\tau$, which similarly begins to decrease before the curve without the application of the error correction code. The curves are cutoff when $\mathcal{Q}/\tau^2 = 1$ for clarity purposes. Additionally, we illustrate the corresponding normalized QFI curves, $\mathcal{Q}/(nt)^2$, in plots (d), (e) and (f) respectively, to emphasize the deviation from the HL.

the t/τth application of error correction, a mixture of GHZ-like states is obtained. Assuming that $\gamma\tau > 0$ and $\omega \neq 0$, it follows that

$$r^2 = e^{-2\gamma\tau}\left(1 + \frac{\gamma}{\Delta}\sin(2\Delta\tau) + \frac{2\gamma^2}{\Delta^2}\sin^2(\Delta\tau)\right) < e^{-2\gamma\tau}\left(1 + \sinh(2\gamma\tau) + \sinh^2(\gamma\tau)\right) = 1, \tag{5.15}$$

consequently, the quantum state becomes more mixed (and less useful for quantum metrology) once the quantity nt/τ becomes very large.

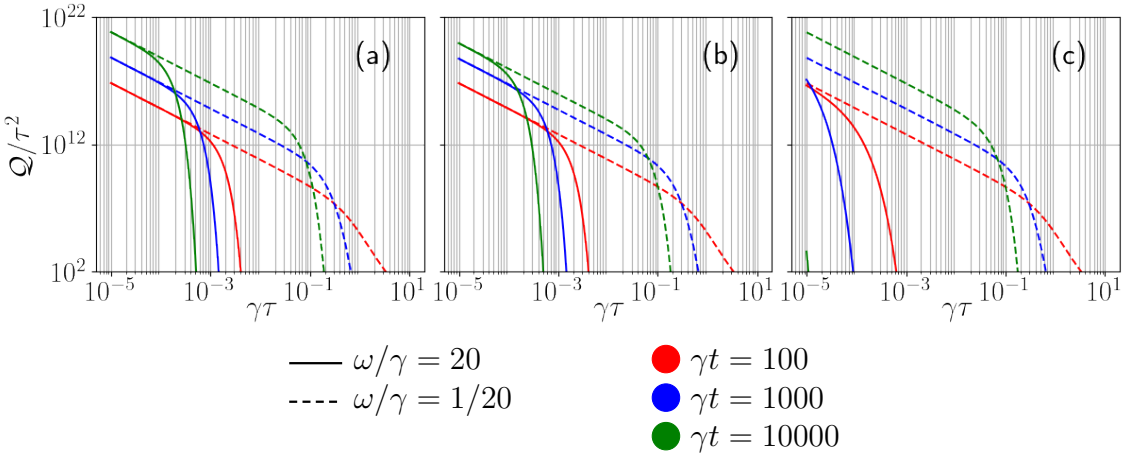


Figure 5.4: An alternative perspective on illustrating the tendencies of $\mathcal{Q}/\tau^2$ for an $n = 25$ qubit GHZ state after repeated applications of error correction. Here, the total sensing time γt is held constant and deviations from the linear curve on the log-log plot represent the QFI tending away from the HL and towards a QFI of zero. The same scenarios are plotted: (a) ideal error correction, (b) a noisy ancilla ($\xi/\gamma = 10^{-4}$), and (c) imperfect syndrome diagnosis ($p = 0.01$). Without any error correction, the QFI after total sensing times $\gamma t = 100, 1000, 10000$ is effectively zero. Note that the three values chosen for the total sensing time, γt, deviate less than the values chosen in Fig. (5.3). This choice was intentional to properly illustrate the scenario of imperfect syndrome diagnosis. Regardless, the curves display here have an analogous curve with similar tendencies displayed in Fig. (5.3).

The QFI of the quantum state in Eq. (5.12) can be written in the form

$$\mathcal{Q}_1 = n^2 t^2 r^{2nt/\tau} f, \tag{5.16}$$

where for small times τ,

$$f = 1 - 2\gamma\tau + \mathcal{O}(\tau^2). \tag{5.17}$$

It is immediately clear that a Heisenberg level of precision is obtained if two conditions are met. The first being that $2\gamma\tau \ll 1$; it was derived in [DCS17; Zho+18] and is equivalent to the constraint for noisy metrology without quantum error correction, Eq. (5.2). The second condition is $r^{2nt/\tau} \approx 1$, which suggests that the HL cannot be maintained indefinitely in a noisy environment (because $r^2 < 1$) and that the QFI will eventually tend to zero. For small τ we have

$$r^{2nt/\tau} = 1 - \frac{4}{3} n(\omega\tau)^2 \gamma t + \mathcal{O}(\tau^3), \tag{5.18}$$

meaning the second condition can be written as $\frac{4}{3}n\omega^2\tau^2\gamma t \ll 1$. This condition goes unnoticed in [DCS17; Zho+18] because it is of second order with respect to τ.

Both of these conditions are illustrated in Fig. (5.3a), Fig. (5.3d) and Fig. (5.4a), where the QFI of an $n = 25$ qubit GHZ state is plotted. In the regime $\omega^2 \gg \gamma^2$ ($\omega/\gamma = 20$), the HL of precision is lost once $r^{2nt/\tau}$ begins to tend to zero.

For each value of r there is a critical value which the exponent will take such that the QFI will begin to rapidly converge to zero. Hence the difference in values of $\gamma\tau$ for when the curves with $\omega/\gamma = 20$ in Fig. (5.3a), Fig. (5.3d) and Fig. (5.4a) deviate from the HL.

In the regime $\omega^2 \ll \gamma^2$ ($\omega/\gamma = 1/20$), the HL level of precision is lost once $\gamma\tau \approx 10^{-2}$, regardless of if $t = 10^3\tau$ or $t = 10^6\tau$. The stark contrast in the families of curves ($\omega^2 \gg \gamma^2$ versus $\omega^2 \ll \gamma^2$) is due to larger deviations from the ideal case when $\omega^2 \gg \gamma^2$. Information about ω is stored in the relative phase, $n\phi t/\tau$, and if an error does occur between applications of error correction, the phase will deviate further from the ideal case. Thus, each round of error correction introduces a small amount of variance to the phase which scales with the magnitude of ω.

In the noisy scenario without error correction, the optimal sensing time (which maximizes the QFI) is $t_{\text{opt}} \approx 1/(n\gamma)$ [Cha+13]. The analogous quantity for the error correction enhanced setting can be computed by first realizing that $\frac{\partial f}{\partial t} = \mathcal{O}(\tau)^2$, therefore the optimal sensing time is obtained by (approximately) maximizing the quantity $t^2 r^{2nt/\tau}$. The resulting optimal sensing time is

$$t_{\text{opt}} = \frac{1}{\frac{2}{3}n\gamma\omega^2\tau^2 + \mathcal{O}(\tau^3)}. \tag{5.19}$$

As expected, t_{opt} increases as τ decreases, and decreases as n increases. The dependence on ω is linked to the effective variance in the phase of the quantum state.

5.5.2 Noisy Ancilla

The inclusion of the noisy ancilla alters the QFI to be

$$\mathcal{Q}_2 = n^2t^2r^{2nt/\tau}(f - g\xi) + \mathcal{O}(\xi^2), \tag{5.20}$$

where g is bounded by

$$\left(\frac{2}{3} - 7\gamma\tau\right)t \leq g + \mathcal{O}(\tau^2) \leq \frac{5}{2}(t + \tau), \tag{5.21}$$

which can be interpreted as another necessary condition to obtain a Heisenberg-like scaling: $\xi t \ll 1$. This is not very surprising, since error correction will becomes less effective as time increases, and ultimately become ineffectual once the ancilla decoheres, $t \approx 1/\xi$. The new condition is displayed in Fig. (5.3b) and Fig. (5.3e), in which the ancillary qubit is set to have a dephasing rate 10000 times weaker than the sensing qubits. The noisy ancilla causes the HL to be lost sooner when compared to the case with a noiseless ancilla. The impact is more pronounced for the curve with $\omega/\gamma = 1/20$ and $t = 10^6\tau$, where the loss of the HL is strictly due to ξt becoming too large instead of $\gamma\tau$. In Fig. (5.4b), where the total sensing time is static (and thus ξt is a constant), the QFI curve with $\gamma t = 10000$ is noticeable shifted when compared to the same curve with ideal error correction in Fig. (5.4a). The problem of noisy ancillary qubits can be overcome by occasionally re-initializing the ancillary qubit (before it becomes too noisy) using an additional layer of error correction.

5.5.3 Imperfect Syndrome Diagnosis

The second hindrance explored is the inclusion of imperfect syndrome diagnosis due to flaws in the error correction hardware. To model this, for each instance of error correction, there is a probability p that the parity measurement between a sensing qubit and the ancillary qubit is incorrect. Hence, if there is a difference parity, then no error correction is performed with probability p. Similarly, if there is no difference in parity (and no correction is needed), there is also a probability p that an unnecessary correction is performed. An unnecessary correction (or lack thereof) will subject the quantum state to additional noise. Furthermore, each round of error correction introduces a small amount of variance to the quantum state due to the imperfect hardware, which will grow as the number of rounds of error correction increases. With the inclusion of imperfect syndrome diagnosis, the QFI is

$$\mathcal{Q}_3 = n^2t^2(rq)^{2nt/\tau}h, \tag{5.22}$$

with

$$q^{2nt/\tau} = 1 - 4p(1-p)\omega^2 t\tau + \mathcal{O}(\tau^2), \tag{5.23}$$

and

$$h = (1-2p)^2 f + 4p\Big(\frac{1-p}{n} + 1 - 2p\Big)\frac{\tau}{t} + \mathcal{O}(\tau^2). \tag{5.24}$$

The inclusion of imperfect syndrome diagnosis makes the true HL unattainable; $\mathcal{Q} \to n^2t^2(1-2p)^2$ as $\tau \to 0$. The multiplicative factor $(1-2p)^2$ is a result of the

added uncertainty from each application of error correction. The exponential term in Eq. (5.22), $(rq)^{2nt/\tau}$, must be approximately equal to 1 to achieve Heisenberg-like precision. This is a more strict version of $r^{2nt/\tau} \approx 1$, and is again due to deviations in the relative phase, which are amplified by the imperfect syndrome diasgnosis. This stronger condition can be seen in Fig. (5.3c), Fig. (5.3f) and Fig. (5.4c), in which the probability of faulty syndrome diagnosis is 1%. The additional condition of $q^{2nt/\tau} \approx 1$ is more pronounced in the regime where $\omega^2 \gg \gamma^2$. The upper bound of precision is displayed in Fig. (5.3f); as $\gamma\tau \to 0$, $\mathcal{Q}/(nt)^2 \to (1-2p)^2 \approx 0.96$.

5.5.4 Fisher Information

Given that the achievable precision of a metrology problem is also constrained by the estimation strategy, a more practical figure of merit is the Fisher information with respect to implementable estimation strategies. Consider measuring the output quantum state, Eq. (5.12), in the basis spanned by $\{|\alpha_+\rangle, |\alpha_-\rangle\}^{\otimes(n+1)}$, in which

$$|\alpha_\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\alpha}|1\rangle), \tag{5.25}$$

and reverse engineering the measurement results to estimate ω. Because of the symmetry of ρ, one only needs to consider the projectors $E_j = |\alpha_+\rangle\langle\alpha_+|^{\otimes n+1-j} |\alpha_-\rangle\langle\alpha_-|^{\otimes j}$, where

$$\mathrm{Tr}\left(E_j\rho\right) = \frac{1+(-1)^j R\cos\left(\theta-\alpha\right)}{2^{n+1}}, \tag{5.26}$$

with $R = r^{nt/\tau}$ and $\theta = n\phi t/\tau$. The Fisher information of this estimation strategy is

$$\mathcal{I} = \sum_j \frac{\mathrm{Tr}\left(E_j\dot{\rho}\right)^2}{\mathrm{Tr}\left(E_j\rho\right)} = \frac{\left(\dot{R}\cos\left(\theta-\alpha\right) - R\dot{\theta}\sin\left(\theta-\alpha\right)\right)^2}{1-R^2\cos\left(\theta-\alpha\right)}, \tag{5.27}$$

where the notation $\dot{\square} = \partial_\omega \square$ is used for conciseness. If α is chosen such that $\cos(\theta-\alpha) \approx 0$, then this estimation strategy approximately saturates the QFI

$$\mathcal{I} = \mathcal{Q} + \mathcal{O}(\tau^2). \tag{5.28}$$

Of course, this requires exact knowledge of ω to implement perfectly, which defeats the purpose of quantum metrology. However, this could be implemented with a high degree of precision using an adaptive estimation strategy [GM05; Fuj06; Wis+09; PJ17]. On a similar note, saturating the QCRB requires that the value of γ is

precisely known. Any uncertainty in the noise model will naturally translate to uncertainty in the estimation of ω. Alternatively, if γ is unknown, one can consider estimating both ω and γ in simultaneity, i.e. consider the setting as a multiparameter quantum metrology problem.

5.5.5 QFI And Entanglement

In **Chapter 3** a relationship between the geometric measure of entanglement G and the QFI is given by [Aug+16]

$$\mathcal{Q}(\rho_\theta) \leq n + 8n^2\sqrt{G(\rho_\theta)}. \tag{5.29}$$

This is an inequality and not an equality because entanglement is a necessary condition and not a sufficient condition [Osz+16]. However, the relationship between QFI and entanglement is much more pronounced for quantum states of the form

$$\rho = \frac{1+R}{2}\left|\psi_+\right\rangle\!\left\langle\psi_+\right| + \frac{1-R}{2}\left|\psi_-\right\rangle\!\left\langle\psi_-\right|, \tag{5.30}$$

with

$$\left|\psi_\pm\right\rangle = \frac{1}{\sqrt{2}}\big(\left|0\right\rangle^{\otimes N} \pm e^{i\theta}\left|1\right\rangle^{\otimes N}\big). \tag{5.31}$$

Hence, ρ is a highly entangled pure state when $R = 1$ and a mixture of two separable states when $R = 0$. Using the recipe for rank-2 mixed symmetric mixed states in [Das+16], the geometric measure of entanglement for the above quantum state is

$$G(\rho) = \frac{1}{2}(1 - \sqrt{1 - R^2}). \tag{5.32}$$

Therefore, the 'quantum part' of the QFI can be written

$$R^2\dot{\theta}^2 = 4G(1-G)\dot{\theta}^2. \tag{5.33}$$

This result, albeit interesting, is mostly a bi-product of the fact that the initialized quantum state was a maximally entangled GHZ state. It is not surprising that the deterioration of the entanglement and the loss of the HL are dependent on the same quantity R^2. In fact, many quantities which measure some aspect of 'quantum-ness' are similarly dependent, such as purity

$$\operatorname{Tr}\rho^2 = \frac{1+R^2}{2}, \tag{5.34}$$

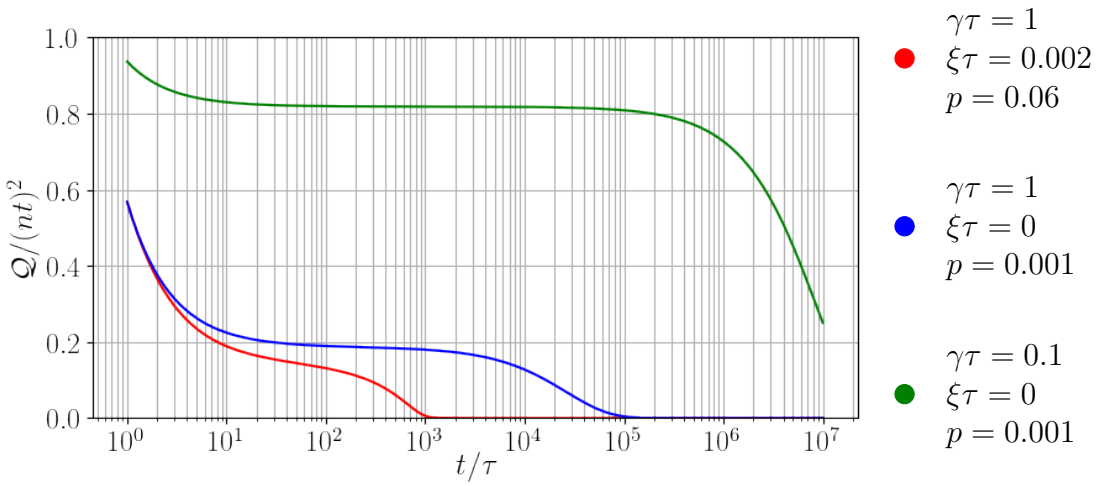


Figure 5.5: Normalized QFI in the small signal regime $\omega/\gamma = 0.01$. ● Today's quantum technologies ($\gamma^{-1} = \tau = 10^{-6}$s, $\xi^{-1} = 5 \times 10^{-4}$s, $p = 0.06$) [Dut+07; Tam+14] suggest a QFI of $\sim$ 20% of the HL can be attained for sensing times $t = 10^1\tau$. ● With improved error correction hardware and a noiseless ancilla, this can be sustained for a sensing time $t = 10^3\tau$. ● The QFI is significantly improved when the rate of error correction is increased by a factor of ten.

and Von Neumann entropy

$$-\operatorname{Tr}\rho\log\rho = -\frac{1+R}{2}\log\left(\frac{1+R}{2}\right) - \frac{1-R}{2}\log\left(\frac{1-R}{2}\right). \tag{5.35}$$

5.6 Current Technologies

In [Dut+07; Tam+14], the electron spin of a nitrogen-vacancy center is entangled to carbon-13 nuclear spins. The nuclear spins act as ancillary qubits, and error correction is performed on the electron spin using the parity check code. The reported dephasing rates are $\gamma^{-1} \sim 10^{-6}$s and $\xi^{-1} \sim 5 \times 10^{-4}$s. The error correction is being performed on a comparable timescale of $\tau \sim 10^{-6}$s, with infidelity reported at $p = 0.06$ [Tam+14]. In Fig. (5.5), this data is used to benchmark the abilities of current error correction technologies as a means of enhancing the precision of a noisy quantum metrology scheme in the regime $\omega^2 \ll \gamma^2$. Because the error correction rate is similar to the dephasing rate, the HL is unattainable. This is still the case with better hardware: $p = 0.001$ and $\xi = 0$ (the latter is justified by regularly re-initializing the ancilla). Notably, if the error correction rate increases by a factor of ten, the achievable QFI is 80% of the HL for a total sensing time of $t = 10^5\tau$. This

greatly outclasses the precision achieved in current experiments [Tay+08; Was+10; Raz+19]. Although this result is promising, it is important to realize that experiments are hindered by more than what is considered in Fig. (5.5), such as parallel noise, imperfect gate fidelity when applying the recovery operations and flaws in the quantum state initialization.

5.7 Other Noise Mitigation Strategies

In striving for an exact solution, it was necessary to consider a specific noise model and a specific error correction protocol. Whereas [DCS17; Zho+18] make no assumptions regarding the noise model. Although a completely general result is more satisfying, it is unfeasible with our methods. Nevertheless, our model and mathematical methodology are easy to adapt. One can substitute any combination of noise model and error correction strategy in place of iid dephasing and the parity check code respectively. In fact, repeated error correction can be forgone entirely and replaced with a suitable quantum control technique [Sek+17], such as dynamical decoupling [Ron+11; SSD16] or reservoir engineering [SW10; Zhe+15].

We conjecture that, just as with discrete applications of the parity check code, for any noise mitigation strategy, the QFI will depend on term similar to $r^{2nt/\tau}$: one which suggests that there exist a critical time where the QFI begins to tend to zero. In fact, using the n qubit bit flip code [Got97] yields the results

$$\mathcal{Q} = n^2 t^2 r^{2nt/\tau} f + \mathcal{O}(\tau^{\frac{n-1}{2}}). \tag{5.36}$$

Hence, for large n the QFI using the bit flip code is effectively the same as if one utilizes the parity check code. The reasoning supporting the aforementioned conjecture is that any errors which occur will cause the relative phase to deviate from the ideal value, and the deviation will remain even after performing a correction. Thus, after each round of error correction, the variance in the phase will increase, which propagates to an increase in variance in the eventual estimate of ω. This conjecture is easily extended to any realistic noise model; as one expects the relative phase to deviate from the ideal value after performing error correction, regardless of the noise model.

We are not suggesting that the parity check code is the most efficient noise mitigation strategy (for transverse noise) at retaining the HL. For example, an adaptive parameter estimation [GM05; Fuj06; Wis+09; PJ17] could be used to supplement

the parity check code by incorporating an unitary operation which approximately corrects the deviations in the relative phase. This strategy is more difficult to implement, as the unitary rotations would be quite small and unlikely to be accurately realizable with current quantum hardware. Indisputably, as quantum technologies continue to improve, and the frequency at which these noise mitigation tools can be applied increases, so too does our ability to maintain the HL for increased sensing times.

5.8 Discussion

Our analysis is in agreement with previous results [DCS17; Zho+18], which suggests that the inequality $2\gamma\tau \ll 1$ is crucial for an error correction enhanced quantum metrology scheme to maintain a Heisenberg-like scaling. However, the findings in [DCS17; Zho+18] are based on the assumption that higher order terms are negligible, $\mathcal{O}(\tau^2) \to 0$, and as a result, Heisenberg-like scaling can be maintained permanently with repeated applications of (arbitrarily fast) error correction. This is not in accordance with today's quantum technologies, as the rate at which error correction can be performed is on a similar order of magnitude to the dephasing rate of physical qubits [Dut+07; Sch+11; Tam+14; Cra+16; Ofe+16]. When the assumption $\mathcal{O}(\tau^2) \to 0$ is discarded, a second necessary condition to maintain the Heisenberg-like scaling emerges, $r^{2nt/\tau} \approx 1 \to \frac{4}{3}n\omega^2\tau^2\gamma t \ll 1$.

Whenever an error occurs, it causes the phase to deviate from the ideal value of $n\omega t$, which is why the HL cannot be maintained indefinitely. That being said, in practise, no quantum metrology requires indefinite sensing time. For spin quibts, a more appropriate upper bound could be the relaxation time, which is typically a few orders of magnitude larger than the dephasing time [Wan+17]. With the limitations of current technologies, Fig. (5.5), this may as well be indefinite.

We specifically analyse the effects of repeated applications of error correction for the specific case when the probe state is initialized in an n qubit GHZ state. A logical generalization is to expand the results to a broader scope of initial states; such as squeezed states [Gro12; ZD14], symmetric states [TA14], or bundled graph states (**Chapter 4**). It is possible that these quantum states (which do not achieve the true HL, but do achieve a quantum advantage and Heisenberg-like scaling) are more robust to the effects of noise and can maintain a quantum advantage for a longer total sensing time when enhanced by error correction.

Further, we chose to analyse a dephasing noise model, something which is more

applicable to atomic systems [SC07; BS13; MFD14; ZYL14]. A future perspective is to consider noise models more relevant to optical systems, such as loss and phase diffusion [Lee+09; Dem+09; KSD11; Zha+13; DJK15]. Error correction codes for continuous variable systems are typically more complex [PZ98; SM05; ZPJ20]; it is not obvious how our results translate to these systems, if at all.

6
Quantum Cryptography for Quantum Metrology

Quantum channels are likely to be the most vulnerable aspect of quantum communication protocols. Without proper cryptographic precautions, a malicious adversary can intercept the information being sent through a quantum channel while the honest parties remain none the wiser. As quantum network sensing and spatially distributed schemes become increasingly popular [Kóm+14; PKD18; Rub+20], it is important to verify which techniques from quantum cryptography are compatible with quantum metrology.

Until very recently, quantum metrology and quantum cryptography were non-overlapping disciplines. Gradually, the idea of security has been introduced to quantum metrology by considering scenarios involving unsecured quantum channels [Xie+18; HMM19], delegated measurements to an untrusted party [Tak+19b; Oka+20; Yin+20], or unwanted eavesdroppers [Kas+21]. Although this direction is new and exciting, the aforementioned references fail to quantify the effects a malicious adversary poses to the quantum metrology problem, i.e the effects on the estimate and its precision. This chapter addresses this problem by linking the cryptographic notion of soundness to an overall uncertainty added to the quantum resource, which propagates to the quantum metrology problem.

In addition to developing a toolbox for the merging of quantum cryptography and quantum metrology, several cryptographic protocols are devised for a variety of cryptographically motivated settings. Such as quantum metrology with an unsecured quantum channel [SMK21] and quantum metrology with delegated tasks [SM]. The protocols devised are completely private, meaning that even if a malicious adversary intercepts the quantum data, they cannot interpret it, and maintain

the integrity of the underlying metrology problem with no more than a quadratic increase in the number of resources. More so, (most of) the protocols devised take into account the limitations of real world quantum hardware and use nothing more complex than local Clifford operations.

6.1 Quantum Cryptography

Cryptography is the practise and study of data security. For a long time, up until the advent of the computer, cryptography was synonymous with encryption - a method to cipher and decipher a message. Without knowledge of the cipher, an adversary could not intercept and learn the contents of the message. Nowadays, in the digital age, cryptography is much more than just encryption, yet the general philosophy of data security remains. Sophisticated techniques are manufactured for a range of tasks, such as sender/receiver authentication, secure data storage, secure computation, et cetera. Cryptography is undeniably essential for safeguarding confidential information and establishing trust between severs in the digital era.

Quantum cryptography is the natural generalization of cryptography where quantum mechanical properties are allowed to be exploited. The quantum framework is accompanied by advantages and disadvantages alike. It is advantageous as quantum systems have built-in security aspects due to the no-cloning theorem and the collapse of the wave function. It is disadvantageous in the fact that an adversary with a quantum computer is much more powerful than an adversary with a classical computer. For example, the modern (classical) RSA encryption scheme is based on the difficulty of factoring large numbers efficiently [RSA78]; this encryption scheme can be broken with Shor's factoring algorithm[1] [Sho94]. As such, quantum cryptography differentiates from classical cryptography in the notion of security. A cryptographic protocol is said to be *computationally secure* if it is immune to an adversary with 'reasonable' computational power and time. Whereas quantum cryptography protocols opt for *unconditionally security*, which is to say that no assumptions are made about the adversaries' computational power and time.

The premise of the first formulation of quantum cryptography [Wie83] was simple but powerful: by randomly encoding the bit '0' ('1') in either $|0\rangle$ ($|1\rangle$) or $|+\rangle$ ($|-\rangle$), then the value of the bit is completely concealed from a malicious adversary if they are not aware of the preparation basis. This result stems from the uncer-

[1] No need for panic; Shor's factoring algorithm is very much out of reach for modern quantum technologies.

tainty principle, Eq. (2.27), which has no classical analogue. This concept paved the way to the famous BB84 protocol for quantum key distribution [BB84]. Since then the applicability of quantum cryptography has thrived [BS16; Pir+20]; for example: quantum money [Aar09; Boz+18], quantum coin flipping [Amb+04; Pap+14], verification of quantum processes [Yin+13; GKK19; ZH19a] and blind quantum computing [BFK09; Bar+12; FK17].

Just as (classical) cryptography is essential for confidentiality and trust in the digital era, so too is quantum cryptography in the quantum era. This is the core idea supporting the integration of quantum cryptography into a quantum metrology problem. If the problem involves multiple parties or communication through a quantum channel, then it is imperative to use quantum cryptography to certify the results and maintain a notion of privacy. Otherwise, a malicious adversary who intercepts an encoded quantum state can either bias the estimation result or estimate the latent parameter themselves. However, the problem is not as simple as using existing cryptographic protocols; in addition to adding security and privacy, the cryptographic protocol must not interfere with the mechanisms of the quantum metrology problem.

6.2 Cryptographic Figures Of Merit

There is no unique cardinal figure of merit for cryptographic protocols due to the sheer vastness of quantum cryptography in both functionality and perspectives. Ergo, a suitable figure of merit for a cryptographic protocol should be relevant to the scope of the protocol and provide a method of comparison between similar protocols. The protocols we devise for quantum metrology take inspiration from quantum message authentication [Bar+02], so it is natural use the same figures of merit: *privacy* and *soundness*. These are both commonly used for most cryptographic protocols whose aim is to verify/authenticate/certify a process. Other than quantum messages [Bar+02], examples include quantum state preparation [ZH19a; ZH19b] and quantum computation [FK17]. Providentially, the soundness of a protocol can be related to the additional bias and uncertainty of the quantum metrology problem.

6.2.1 Privacy

Privacy is a straightforward concept which quantifies the amount of information a malicious eavesdropper can extract from a message (quantum or otherwise). The

protocols outlined in this chapter are all *completely private*, this is to say that an eavesdropper can extract no information. If an eavesdropper can access the quantum state ρ_E, then this is achieved if

$$\mathbb{E}(\rho_E) = \mathbb{I}/d, \tag{6.1}$$

where d is the dimension of ρ_E. Thus, a protocol is completely private when the expected quantum state accessible to an eavesdropper is indistinguishable from the maximally mixed state.

Having a completely private protocol is paramount for quantum metrology, as this prevents an eavesdropper from learning anything about the unknown parameter for themselves. This was overlooked in the first work which established the idea of quantum metrology integrated into a cryptographic framework [HMM19], in the appendix of [SMK21] we show that their protocol is not completely private and that an eavesdropper can go completely undetected while learning performing parameter estimation for themselves.

6.2.2 Soundness

For authentication schemes, the soundness of a cryptographic protocol is the standard figure of merit used to judge the security of a protocol [Bar+02]. In essence, the soundness of a protocol quantifies the ability of a malicious adversary to alter the quantum state whilst remaining undetected. The formal mathematical definition of soundness varies depending on the formulation of the cryptographic protocol [Bar+02; FK17; ZH19a; Tak+19a], and is sometimes referred to as verifiability [GKK19]. The version used in the work presented in this thesis uses a slightly modified version of the definition presented in [Bar+02].

Authentication schemes have two outputs: a binary accept or reject clause as well as a quantum output. The quantum output varies as per the protocol, in this chapter, it will either be a quantum state or a measurement result. The protocols are also equipped with ancillary qubits, which are constructed to have a deterministic measurement outcome in an ideal scenario in which there is no malicious activity. If the expected measurement result is observed, the outcome of 'accept' is assigned. However, if an unexpected result is observed, then it must be the result of malicious activity, and the outcome of 'reject' is assigned. For the sake of unconditional security, no assumptions are made with respect to the computational power of a malicious adversary. More so, it is assumed that a malicious adversary is completely

familiar with the inner mechanisms of the protocol. In order to dissuade a malicious adversary, the protocols are supported by a set of classical keys $\mathcal{K}$, where each key alters the protocol differently. Before implementing a protocol, a key is chosen at random, and even if a malicious adversary may have access to the set of possible keys, it is assumed that they do not have access to the random choice. If there are multiple trusted parties who need access to the key, it is assumed that the key can be shared securely. This can be accomplished through a secure classical channel or quantum key distribution [BB84]. For all intents and purposes we assume that a malicious adversary cannot access the (random) choice classical key.

The mathematical definition of soundness is a bound on the probability of witnessing 'accept', while the quantum output, ρ_{out} is simultaneously far from the ideal ρ_{id}. In [Bar+02], the protocol is constructed for ρ_{id} being a pure state, and the 'distance' is recorded in $1 - \text{Tr}(\rho_{\text{id}}\rho_{\text{out}})$. In [SM], the outputs are not necessarily pure states, and we generalize the 'distance' as $1 - \mathscr{F}(\rho_{\text{id}}, \rho_{\text{out}})$. Both expressions are equivalent in the event that ρ_{id} is a pure state. Mathematically, a protocol has soundness δ if

$$\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}} p_{\text{acc}}(k,\Gamma)\cdot\Big(1-\mathscr{F}\big(\rho_{\text{id}},\rho_{\text{out}}(k,\Gamma)\big)\Big)\leq\delta. \tag{6.2}$$

Here, Γ represents any possible attack a malicious adversary may perform, and $k \in \mathcal{K}$ is the specific key chosen. The probability of the protocol outputting 'accept', $p_{\text{acc}}(k,\Gamma)$, and the output $\rho_{\text{out}}(k,\Gamma)$ are dependent on both of these quantities. A well designed protocol should be provide a sense of security for all malicious attacks, thus Eq. (6.2) must hold for all Γ.

When it can be written that $p_{\text{acc}}(k,\Gamma) \geq \alpha$, then Eq. (6.2) can be transformed into the inequality

$$1-\mathbb{E}\Big(F\big(\rho_{\text{id}},\rho_{\text{out}}\big)\Big)\leq\frac{\delta}{\alpha}, \tag{6.3}$$

where the dependence of ρ_{out} on the key k and the attack Γ has been omitted for clarity. The quantity α is sometimes referred to as the statistical significance [ZH19a]. This alternative formulation permits more easily permits the use of other common figures of merit which are intertwined with the soundness and statistical significance [ZH19a; ZH19b]. More so, it will be shown that Eq. (6.3) can be manipulated to determine the utility of ρ_{out} for quantum metrology. This is done by bounding the trace distance, which can be found using the the Fuchs-van de Graaf inequalities

[FV99], Eq. (2.35), and the arithmetic-quadratic mean inequality

$$\mathbb{E}\Big(\mathscr{D}\big(\rho_{\text{id}},\rho_{\text{out}}\big)\Big) \leq \sqrt{\mathbb{E}\Big(\mathscr{D}\big(\rho_{\text{id}},\rho_{\text{out}}\big)^2\Big)} \leq \sqrt{1-\mathbb{E}\Big(F\big(\rho_{\text{id}},\rho_{\text{out}}\big)\Big)} \leq \sqrt{\frac{\delta}{\alpha}}. \tag{6.4}$$

6.3 Cryptographic Quantum Metrology

The first adaptation of a quantum metrology problem in a cryptographic framework can be found in [Kóm+14]. In the article, an entangled state is distributed from a central node to several exterior nodes, where a local phase is encoded and sent back to the central node for phase estimation. The authors propose occasionally distributing non-entangled decoy qubits throughout the sensing network. These decoy qubits have a deterministic measurement and are used to detect and thwart malicious activity. As this was not focal point of [Kóm+14], the 'proof' of security is substandard, nonetheless the protocol was a good starting point for a cryptographic framework of quantum metrology.

The concept was later picked up in [HMM19], where two honest parties wish to perform phase estimation over an unsecured quantum channel. Alice sends a non-encoded quantum state to Bob, who encodes a phase using a unitary, and sends the quantum state back to Alice to be measured. The quantum states are sent back and forth through an unsecured quantum channel. The authors of [HMM19] suggest a simple protocol to prevent a malicious adversary from intercepting the channel and tampering with the results. In each use of the quantum channel, Alice randomly prepares one of four quantum states: either a decoy quantum state $|0\rangle^{\otimes n}$ or $|1\rangle^{\otimes n}$, which will not serve any utility for phase estimation, or a GHZ state $|\psi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$ or $|\psi_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} - |1\rangle^{\otimes n})$. Additionally, Bob will either randomly encode the unknown phase θ, or a phase ϕ which maps $|\psi_\pm\rangle$ to $|\psi_\mp\rangle$. Even though this protocol is more sophisticated than what was presented in [Kóm+14], we show in [SMK21] that it is vulnerable to a malicious attack which is undetectable by Alice and Bob. Additionally, [HMM19] and many others who have since investigated 'cryptographic quantum metrology' [Xie+18; Tak+19b; Oka+20; Yin+20; Kas+21] fail to elaborate on the ramifications on the underlying metrology problem.

In a cryptographic framework, many of the concepts from estimation theory discussed in **Chapter 3** have to be altered in some capacity. This is because there is no guarantee that the resource used for the parameter estimation problem is the ideal resource. To fit the language of statistics, the cryptographic framework of quantum metrology injects uncertainty into the estimate. This additional uncertainty can

be bounded by taking proper precautions and employing appropriate cryptographic protocols. However, this uncertainty in the resource leads to ambiguity with respect to the construction of an estimator; it is not immediately obvious how to select a measurement or how to process the measurement data. Assuming that the additional uncertainty is small, the most straightforward strategy is to process the data as if it was the ideal resource. Evidently, the unbiased condition, Eq. (3.1), is not necessarily satisfied. Since an unbiased estimator is integral to saturate the CRB, the QFI would be a naive choice of a figure of merit for quantum metrology within a cryptographic framework. Instead, we introduce the concept of *integrity* in [SMK21] as a figure of merit. Integrity refers to the ability of a cryptographic protocol to retain the quantum state and functionality in the presence of malicious adversaries. In this chapter, the notation $\square'$ is used to signify the quantity $\square$ in a cryptographic framework. For example, $\hat{\theta}$ is an estimator with a MSE of $\Delta^2\hat{\theta}$ in an ideal framework and $\hat{\theta}'$ is an estimator with a MSE of $\Delta^2\hat{\theta}'$ in the cryptographic framework. The integrity of the cryptographic quantum metrology problem is measured in two ways, the first is the added bias

$$\left|\mathbb{E}(\hat{\theta}') - \mathbb{E}(\hat{\theta})\right|, \tag{6.5}$$

and the second is the increase in the MSE

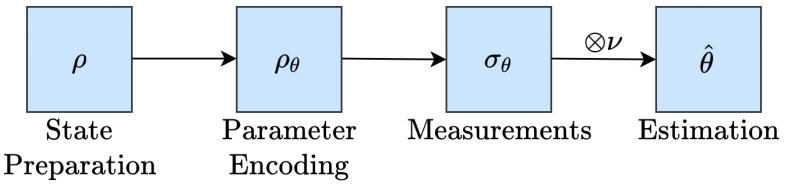
$$\left|\Delta^2\hat{\theta}' - \Delta^2\hat{\theta}\right|. \tag{6.6}$$

For simplicity, we restrict estimation strategies, in which the value of the unknown parameter is inferred from expectation value of an observable O. The specific details of this strategy can be found in **Chapter 3**.

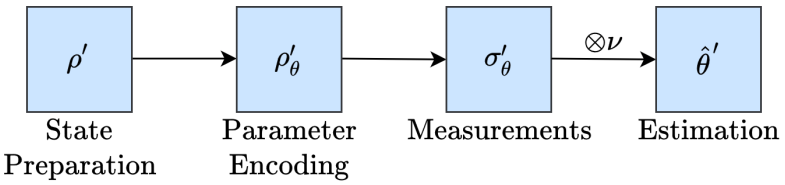
6.3.1 Bounding The Integrity

As Fig. (6.1) suggests, a quantum metrology problem can be altered at many stages of the estimation process by a malicious adversary: state preparation, parameter encoding, or the measurements. Because the measurement is the final 'quantum step' in the process before creating the estimate, the measurement statistics in the cryptographic framework must resemble the measurement statistics in the ideal framework. Otherwise, the estimate would not be practical.

Even though measurement results are a classical quantity, the measurement statistics can always be written as a mixed state with no coherence terms, where the amplitudes correspond to probabilities of witnessing a certain measurement outcome. If the observable the estimate is being inferred from has an eigenbasis with



(a) Quantum Metrology in an Ideal Framework.



(b) Quantum Metrology in a Cryptographic Framework.

Figure 6.1: Comparison between a quantum metrology problem in an ideal framework (sans malicious adversary) and a cryptographic framework (potentially a malicious adversary). In the ideal framework (a), a quantum state ρ is prepared, then an unknown parameter is encoded into the quantum states through a CPTP map $\rho_\theta = \Lambda_\theta(\rho)$, finally a measurement $\mathcal{M}$ is performed on the encoded quantum state. After ν repetitions, the measurement results are used to construct an estimate $\hat{\theta}$. In the cryptographic framework (b), a malicious adversary can intercept and alter the process at any step of the problem. For example, the state preparation can be done by an untrusted source, or an unsecured quantum channel may be intercepted. In fact, the subscript θ in the cryptographic framework is somewhat misleading as there is no guarantee that either ρ'_θ or σ'_θ is dependent on θ. Additionally, the assumption of an iid process is discarded in the cryptographic framework: ρ' in the first round may be different from the ρ' in the second round (or any other round). Note that this figure depicts a completely general cryptographic setting, while the latter sections of this chapter explore specific cryptographic settings, in which it will be clear how and when a malicious adversary may alter the quantum metrology problem.

projectors $\{E\}$, then the corresponding measurement statistics of an encoded quantum state ρ_θ is

$$\mathcal{M}(\rho_\theta) = \sum_E E\rho_\theta E. \tag{6.7}$$

For example if $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is measured with respect to the computational basis, then the measurement statistics are $\mathcal{M}(|\psi\rangle) = |\alpha|^2 |0\rangle\langle 0| + |\beta|^2 |1\rangle\langle 1|$. Similarly, the measurement statistics in a cryptographic framework can always be derived from an

arbitrary (not necessarily encoded) quantum state ρ'_θ. Mathematically, we demand that

$$\frac{1}{\nu}\sum_{j=1}^{\nu}\mathscr{D}\big(\mathcal{M}(\rho_\theta),\mathcal{M}(\rho_\theta^{\prime(j)})\big)\leq\varepsilon\ll 1, \tag{6.8}$$

where $\rho_\theta^{\prime(j)}$ is a quantum state which outputs the measurement statistics of the jth round of the prepare, encode and measure portion of the quantum metrology problem in the cryptographic framework. Eq. (6.3) and Eq. (6.4) suggests that this can be achieved by implementing appropriate cryptographic protocols.

Suppose that the measurements are done in a secure fashion without malicious interference. If the encoded quantum states in the cryptographic framework obey the analogous restriction

$$\frac{1}{\nu}\sum_{j=1}^{\nu}\mathscr{D}\big(\rho_\theta,\rho_\theta^{\prime(j)}\big)\leq\varepsilon\ll 1, \tag{6.9}$$

then Eq. (6.8) will still hold because of the monotonicity of the trace distance, Eq. (2.33),

$$\mathscr{D}\big(\mathcal{M}(\rho_\theta),\mathcal{M}(\rho_\theta^{\prime(j)})\big)\leq\mathscr{D}\big(\rho_\theta,\rho_\theta^{\prime(j)}\big). \tag{6.10}$$

The same argument holds if the malicious interference is localised to the state preparation step in Fig. (6.1b). In fact, Eq. (6.9) was the imposed inequality in [SMK21], however, we needed to generalize to Eq. (6.8) in [SM] because we explore the possibility of delegating the measurement step to an untrusted party. In either case, the trace distance was chosen because of the relationship to distance of resulting classical probability distributions, Eq. (2.32): if ε is small, then any measurement will give rise to similar probability distributions [NC02].

To properly gauge the effects of a malicious adversary, we examine a specific estimation strategy. We revisit that which was established in **Chapter 3**: inferring an estimate from an observable. That is, the expectation value of the observable O is estimated and then inverted. This strategy was chosen due to the mathematical simplicity and for the fact that it can be used to saturate the HL. In the ideal framework, this initial estimate is labelled $\hat{f}$. Specifically

$$\hat{f}=\frac{1}{\nu}\sum_{j=1}m_j, \tag{6.11}$$

where m_j is the eigenvalue associated to the jth measurement result, where $\mathbb{E}(m_j)=\mathrm{Tr}(O\rho_\theta)$. This is equivalent to $\mathbb{E}(m_j)=\mathrm{Tr}\left(O\mathcal{M}(\rho_\theta)\right)$. In the cryptographic frame-

work, the analogous estimate is constructed

$$\hat{f}' = \frac{1}{\nu}\sum_{j=1} m'_j, \tag{6.12}$$

where $\mathbb{E}(m'_j) = \mathrm{Tr}\left(O\mathcal{M}(\rho_\theta'^{(j)})\right)$, which is then inverted as if it were the ideal framework. Assuming that ε is sufficiently small, the first order Taylor expansion of $f^{-1}(\hat{f}')$

$$\hat{\theta}' = \theta + \frac{1}{\frac{\partial\langle O\rangle}{\partial\theta}}(\hat{f}' - \langle O\rangle) \tag{6.13}$$

provides a valid approximation even in the cryptographic framework. Here, $\langle O\rangle$ is the expectation value with respect to the ideal framework, thus $\langle O\rangle = \mathrm{Tr}(O\rho_\theta)$. Eq. (6.13) suggests that in the cryptographic framework, the added bias is bounded by

$$\begin{aligned}
\left|\mathbb{E}(\hat{\theta}') - \mathbb{E}(\hat{\theta})\right| &= \frac{1}{\left|\frac{\partial\langle O\rangle}{\partial\theta}\right|}\left|\mathbb{E}(\hat{f}') - \mathbb{E}(\hat{f})\right| \\
&= \frac{1}{\nu\left|\frac{\partial\langle O\rangle}{\partial\theta}\right|}\Big|\sum_{j=1}^{\nu}\mathrm{Tr}\left(O\mathcal{M}(\rho_\theta'^{(j)}) - O\mathcal{M}(\rho_\theta)\right)\Big| \\
&\leq \frac{2o}{\nu\left|\frac{\partial\langle O\rangle}{\partial\theta}\right|}\sum_{j=1}^{\nu}\mathscr{D}\big(\mathcal{M}(\rho_\theta), \mathcal{M}(\rho_\theta'^{(j)})\big) \\
&\leq \frac{2o\varepsilon}{\left|\frac{\partial\langle O\rangle}{\partial\theta}\right|},
\end{aligned} \tag{6.14}$$

where o is the maximum magnitude of the eigenvalues of O. Recall from **Chapter 3** that in the ideal framework

$$\Delta^2\hat{f} = \frac{\mathrm{Tr}(O^2\rho_\theta) - \mathrm{Tr}(O\rho_\theta)^2}{\nu} = \frac{\mathrm{Tr}(\mathbf{O}\rho_\theta\otimes\rho_\theta)}{\nu}, \tag{6.15}$$

where $\mathbf{O} = O^2\otimes\mathbb{I} - O\otimes O$. Note that the maximum magnitude of the eigenvalues of $\mathbf{O}$ is bounded below $2o^2$. In the cryptographic framework, the MSE is the sum of the variance and the square of the bias

$$\begin{aligned}
\Delta^2\hat{f}' &= \mathbb{E}\big((\hat{f}' - f)^2\big) \\
&= \mathbb{E}\big(\hat{f}' - \mathbb{E}(\hat{f}')\big)^2 + \big(\mathbb{E}(\hat{f}') - f\big)^2 \\
&\leq \frac{1}{\nu^2}\sum_{j=1}^{\nu}\mathrm{Tr}\left(\mathbf{O}\mathcal{M}(\rho_\theta'^{(j)})\otimes\mathcal{M}(\rho_\theta'^{(j)})\right) + 4o^2\varepsilon^2.
\end{aligned} \tag{6.16}$$

It follows that the increase of the MSE is bounded by

$$\begin{aligned}\left|\Delta^2\hat{\theta}' - \Delta^2\hat{\theta}\right| &= \frac{1}{|\frac{\partial\langle O\rangle}{\partial\theta}|^2}\left|\Delta^2\hat{f}' - \Delta^2\hat{f}\right| \\ &\leq \frac{4o^2}{\nu^2|\frac{\partial\langle O\rangle}{\partial\theta}|^2}\sum_{j=1}^{\nu}\mathscr{D}\big(\mathcal{M}(\rho_\theta)\otimes\mathcal{M}(\rho_\theta), \mathcal{M}(\rho_\theta^{\prime(j)})\otimes\mathcal{M}(\rho_\theta^{\prime(j)})\big) + \frac{4o^2\varepsilon^2}{|\frac{\partial\langle O\rangle}{\partial\theta}|^2} \\ &\leq \frac{8o^2\nu^{-1}\varepsilon + 4o^2\varepsilon^2}{|\frac{\partial\langle O\rangle}{\partial\theta}|^2},\end{aligned} \tag{6.17}$$

where the triangle inequality

$$\mathscr{D}(\rho_1\otimes\rho_1, \rho_2\otimes\rho_2) \leq \mathscr{D}(\rho_1\otimes\rho_1, \rho_1\otimes\rho_2) + \mathscr{D}(\rho_1\otimes\rho_2, \rho_2\otimes\rho_2) = 2\mathscr{D}(\rho_1, \rho_2) \tag{6.18}$$

is used in the derivation of Eq. (6.17).

Notice that as $\nu \to \infty$, the added bias in Eq. (6.14) does not vanish, and as a consequence, neither does the increase in the MSE, Eq. (6.17). This is due to the construction of the cryptographic framework, where Eq. (6.8) can be interpreted as an average amount of uncertainty in the measurement statistics. If the uncertainty in each round is constant, ε is of course independent of ν, which ultimately limits the achievable precision of the quantum metrology problem. For the functionality of said quantum metrology problem to be the same in the cryptographic framework when compared to the ideal framework, $\Delta^2\hat{\theta}'$ must scale similarly to $\Delta^2\hat{\theta}$. This is equivalent to the difference in the MSE scaling similarly to $\Delta^2\hat{\theta}$, which occurs when

$$\varepsilon^2 \leq \nu^{-1}. \tag{6.19}$$

The factor of $4o^2$ is ignored as it is dependent on the metrology portion of the problem whereas ε is dependent on the cryptographic portion of the problem. The term $8o^2\nu^{-1}\varepsilon$ term is ignored, as it is appropriately small if $\varepsilon^2 \leq \nu^{-1}$.

It follows from the equations for the added bias and difference in MSE, Eq. (6.14) and Eq. (6.17) respectively, along with the relationship between trace distance and soundness, Eq. (6.4), that if a cryptographic protocol has soundness δ and statistical significance α, then the integrity of the quantum metrology problem is represented by the added bias

$$\left|\mathbb{E}(\hat{\theta}') - \mathbb{E}(\hat{\theta})\right| \leq \frac{2o}{|\frac{\partial\langle O\rangle}{\partial\theta}|}\sqrt{\frac{\delta}{\alpha}}, \tag{6.20}$$

and the the increase in the MSE

$$\left|\Delta^2\hat{\theta}' - \Delta^2\hat{\theta}\right| \leq \frac{4o^2}{|\frac{\partial\langle O\rangle}{\partial\theta}|^2}\left(2\nu^{-1}\sqrt{\frac{\delta}{\alpha}} + \frac{\delta}{\alpha}\right). \tag{6.21}$$

More so, Eq. (6.19) suggests that the effective functionality is retained when

$$\frac{\delta}{\alpha} \leq \nu^{-1}. \tag{6.22}$$

It should be noted that the trace distance and soundness relationship, Eq. (6.4), and the demanded proximity of the average measurement statistics, Eq. (6.8), are not a function of the same quantities. The former is a function of the expected trace distance while the latter is simply the trace distance. This is because a metrology problem is designed for specific states, while it is atypical for a cryptography protocol to have a precise output. Although these ideologies may seem to contrast with each other, we propose two solutions to remedy the difference. The first is that the measurement statistics of each round can be interpreted as the average measurement statistics after implementing the protocol, from which the integrity relationships still hold because of the strong convexity of trace distance [NC02]

$$\mathscr{D}\big(\rho_{\text{id}}, \mathbb{E}(\rho_{\text{out}})\big) \leq \mathbb{E}\big(\mathscr{D}(\rho_{\text{id}}, \rho_{\text{out}})\big). \tag{6.23}$$

The second, is that for sufficiently large ν, the law of large numbers dictates that the proximity of the average measurement statistics will tend towards the expected value

$$\frac{1}{\nu}\sum_{j=1}^{\nu} \mathscr{D}(\sigma_\theta, \sigma_\theta'^{(j)}) \approx \mathbb{E}\big(\mathscr{D}(\sigma_\theta, \sigma_\theta')\big). \tag{6.24}$$

6.4 Quantum Metrology Over An Unsecured Quantum Channel

The first cryptographic setting established in this chapter is when the quantum metrology problem uses an unsecured quantum channel [SMK21]. In quantum sensing networks, the quantum channels will likely be the most vulnerable to malicious attacks [Kóm+14], so it important to include a cryptographic protocol to carry out the metrology problem in a secure fashion. This was the basis of the work presented in [HMM19], however, as described above, the authors fail to create a secure

protocol. To achieve a notion of security, the protocols presented in this section take inspiration from quantum authentication schemes [Bar+02; BW16]. Quantum authentication schemes are cryptographic protocols designed to send quantum states across an unsecured quantum channel in a private and secure fashion, which is precisely the nature of the task at hand.

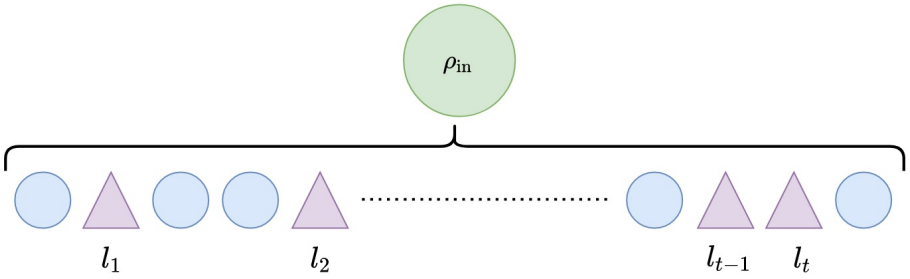
6.4.1 The Protocols

Two protocols are presented for the task of quantum metrology over an unsecured quantum channel: i) a modified version of the trap code [BGS13], and ii) a modified version of the Clifford code [Aha+17]. From a functional stand point the two protocols are nearly identical, however the encryption and decryption methods vary drastically from a complexity standpoint and ease of implementation. The encryption scheme for the trap code is restricted to locally acting Clifford operations, $C \in \mathcal{C}_1^{\otimes m}$. In contrast, the encryption scheme for the Clifford code is an arbitrary $C \in \mathcal{C}_m$. As expected, the Clifford code leads to a much stronger soundness statement, due to the additional entanglement gained from the encryption.

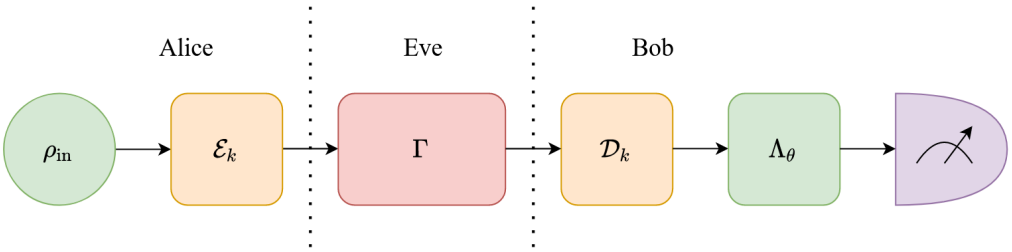
In this setting, Alice and Bob are the trusted parties who wish to execute a quantum metrology problem. They are separated by an unsecured quantum channel, which may be intercepted by a malicious eavesdropper, labelled Eve. Note that Alice and Bob share a secure classical channel to communicate classical information, such as the choice of the random key. This is a standard assumption in quantum cryptography.

To have the ability to detect Eve, Alice prepares an input state ρ_{in}, which is a combination of the quantum state intended for the metrology problem ρ_{id}, as well as t ancillary flag qubits. An example of an input state is depicted in Fig. (6.2a). The flag qubits are all initialized in the state $|0\rangle$, and upon receipt Bob measured the flag qubits in the computational basis. In an ideal setting, the measurement will ubiquitously witness the result $|0\rangle^{\otimes t}$; any other result suggests that the quantum channel was compromised. This deterministic measurement result aids in certifying whether or not Eve tampered with the quantum channel.

After preparing the input state ρ_{in}, Alice encrypts it using a random Clifford operation. The set from which the Clifford operation is chosen from is dependent on the protocol. Upon receipt, Bob decrypts the quantum state by applying the inverse operation applied by Alice. Bob then measures the ancillary flag qubits in computational basis. If the expected measurement result $|0\rangle^{\otimes t}$ is witnessed, Bob will utilize the remaining qubits for the quantum metrology problem, otherwise they are



(a) Initialized quantum state before using the unsecured quantum channel.



(b) Schematic of the protocols.

Figure 6.2: (a) Alice prepares the quantum state ρ_{in}, which is a combination of t ancillary flag qubits (randomly positioned) as well as the quantum state ρ intended for quantum metrology. The flag qubits are indexed at positions $l_1, l_2, \ldots, l_t$. (b) Before utilizing the quantum channel, Alice and Bob randomly select a classical key k. This classical key corresponds to the encryption operation ($\mathcal{E}_k$) performed by Alice, and the decryption operation ($\mathcal{D}_k = \mathcal{E}_k^\dagger$) performed by Bob upon receipt. A malicious eavesdropper, labeled Eve, has complete access to the quantum quantum channel. Without loss of generality, Eve can perform any CPTP map Γ when interacting with the channel. Bob encodes the unknown parameter into the portion of the quantum state intended for quantum metrology. Finally, Bob measures the qubits accordingly: the ancillary flag qubits in the computational basis, and the metrology qubits in the appropriate basis to construct an estimate. If the flag qubit measurement is an unexpected output, then a malicious adversary must have tampered with the quantum channel.

discard the quantum state as Eve must have tampered with the quantum channel. This process is illustrated in Fig. (6.2b).

Implementation Instructions:

1. Prior to using the quantum channel, Alice and Bob randomly select a key $k \in \mathcal{K}$, which is linked to an encryption operator $\mathcal{E}_k$. Specific to trap code, the key also contains information about a tuple $\ell = (l_1, \ldots, l_t)$ of length t, this

tuple contains the index locations of the ancillary flag qubits.

   (a) For the trap code, $\mathcal{E}_k \in \mathcal{C}_1^{\otimes m}$.
   (b) For the Clifford code, $\mathcal{E}_k \in \mathcal{C}_m$.

2. Alice creates the $m = n + t$ qubit state ρ_{in} by inserting t ancillary flag qubits $|0\rangle$ at the positions indexed by ℓ, and the remaining n qubit state ρ is the quantum state designated for quantum metrology.

   (a) For the trap code, it is important that ℓ is randomly chosen because the encryption operation does not generate entanglement.
   (b) For the Clifford code, ℓ can be static. This is because the encryption will generate entanglement between the ancillary qubits and the rest of the quantum state.

3. Alice encrypts the input state by applying the Clifford operator $\mathcal{E}_k$ and sends the quantum state to Bob.

4. Upon receipt, Bob decrypts the quantum state by applying the inverse operator $\mathcal{E}_k^\dagger$ upon receipt.

5. Bob measures the ancillary flag qubits in the computational basis. The result is accepted if $|0\rangle\langle 0|^{\otimes t}$ is measured. The quantum state is discarded otherwise.

6. If the result is accepted, Bob continues with the quantum metrology problem using the remaining qubits.

The random choice of encryption operation makes it impossible for Eve to extract any information about ρ_{in}, meaning that protocols are completely private. To see explicitly why, consider ρ_{in} in the Pauli basis

$$\rho_{\text{in}} = \frac{1}{2^m} \sum_{P \in \mathcal{P}_m} \text{Tr}(P\rho_{\text{in}}) P. \tag{6.25}$$

Using the Clifford code, the expected quantum state available to Eve is

$$\mathbb{E}(\rho_E) = \frac{1}{2^m |\mathcal{C}_m|} \sum_{C \in \mathcal{C}_m} \sum_{P \in \mathcal{P}_m} \text{Tr}(P\rho_{\text{in}}) CPC^\dagger. \tag{6.26}$$

For every $P \neq \mathbb{I}$, the Clifford group can be partitioned into pairs of operators (C_a, C_b) such that $C_a P C_a^\dagger = -C_b P C_b^\dagger$, hence the only-non vanishing term is $P = \mathbb{I}$,

and thus Eve cannot distinguish the quantum state from the maximally mixed state. For the trap code, the Pauli and Clifford operations can be decomposed into local operations, $C = \bigotimes_{j=1}^{m} C_j$ and $P = \bigotimes_{j=1}^{m} P_j$. Here, the expected quantum state available to Eve is

$$\mathbb{E}(\rho_E) = \frac{1}{2^m |\mathcal{C}_1|^m} \sum_{C \in \mathcal{C}_1^{\otimes m}} \sum_{P \in \mathcal{P}_m} \mathrm{Tr}(P \rho_{\mathrm{in}}) \bigotimes_{j=1}^{m} C_j P_j C_j^\dagger. \tag{6.27}$$

By the same intuition, the only non-vanishing term is when P is identically the identity, and thus using the trap Code, Eve cannot distinguish the quantum state from the maximally mixed state. Even though no information about the unknown parameter with respect to the metrology problem is passed through the quantum channel, as per Fig. (6.2b), having complete privacy is still important. The same protocol can be used in the nearly identical setting where it is Alice who encodes the unknown parameter. More so, it will be shown that the protocol can be extended to a setting where Alice and Bob use the same quantum channel twice, similar to the setting of [HMM19]. In either of these two settings, having a completely private protocol prevents Eve from extracting information about the unknown parameter in question.

Privacy is achieved as a consequence of randomly sampling $\mathcal{E}_k$ from a large set of Clifford operations. For example, the set $\mathcal{C}_1^{\otimes m}$ has 24^m elements. Although we do not focus on the logistics of the classical channel in our protocol, it is important to acknowledge that the size of the classical key required is quite large. As an alternative, one can consider sampling $\mathcal{E}_k$ from a smaller set of $\mathcal{O}(m2^m)$ unitary operators, which approximately guarantees privacy [Hay+04]. Although in doing so, other assumptions are needed, namely that Eve not having access to a quantum memory [LL15].

A derivation for the soundness[2] of the two protocols can be found in **Appendix C**, in which it is shown that the soundness of the trap code is $\delta_{\mathrm{trap}} = \frac{3n}{2t}$, and the soundness of the Clifford code is $\delta_{\mathrm{Cliff}} = \frac{1}{2^t}$. Eq. (6.22) states that the integrity of the underlying metrology problem is maintained when $\frac{\delta}{\alpha} \leq \nu^{-1}$. Equivalently, the number of ancillary flag qubits required is $t_{\mathrm{trap}} \geq \frac{3n\nu}{2\alpha}$ for the trap code, and $t_{\mathrm{Cliff}} \geq \log_2 \frac{\nu}{\alpha}$ using the Clifford code. In the ideal framework, the total number of qubits is νn, in the cryptographic framework it is $\nu(n+t)$. This is a quadratic

[2]We derive the soundness with the assumption that the quantum state intended for quantum metrology, ρ_{id}, is a pure state, because this greatly simplifies the derivation. This is a logical assumption since pure states are superior resources for quantum metrology.

increase in resources if using the trap code, and a log-linear increase in resources if using the Clifford code.

6.4.2 Generalizations

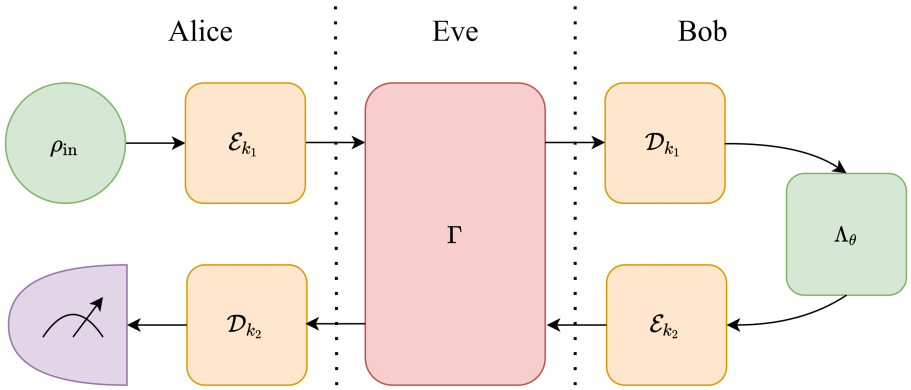


Figure 6.3: In the extended version of the protocol, the unsecured quantum channel is used twice. Alice sends the quantum state ρ_{in} to Bob to be encoded, after which it is sent back to Alice. Because the quantum channel is used twice, the classical key shared by Alice and Bob describes the encryption and decryption operation for the first use of the quantum channel $(\mathcal{E}_{k_1}, \mathcal{D}_{k_1})$ and the second use of the quantum channel $(\mathcal{E}_{k_2}, \mathcal{D}_{k_2})$.

The work in [HMM19] addresses the distribution of entangled resources over quantum channels for quantum metrology, however, with a more restricted Bob, so that the measurement is also left to Alice, requiring the state be sent back to Alice once Bob has done the encoding. Both the trap code and Clifford code can be easily adapted to this setting. To do so, Alice and Bob perform a second encryption operation before the second usage of the quantum channel. The generalization of the protocol is illustrated in Fig. (6.3). Using two encryption operations is imperative for the success of the protocol; if it was just Alice who performed the encryption and the decryption, then Eve could simply apply a unitary on the use of the quantum channel, and its inverse on the second usage. This will not alter any of the ancillary flag qubits but can bias the qubits intended for quantum metrology. In **Appendix C**, the soundness of the generalized protocols are computed to be $\delta_{\text{trap}} = \frac{9n}{4t}$ and $\delta_{\text{Cliff}} = \frac{1}{2^t}$.

An alternative generalization is a multipartite setting, depicted in Fig. (6.4). This would be a practical tool for any quantum sensing network problem [Kóm+14; PKD18; Rub+20] with unsecured quantum channels. Here a central node $\mathcal{N}_0$ is

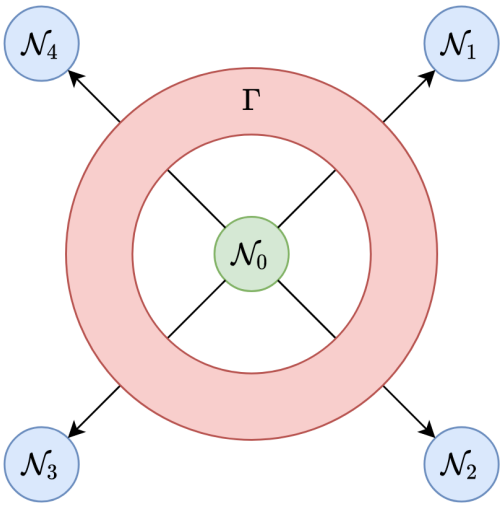


Figure 6.4: Generalization to a multipartite framework, where a central node $\mathcal{N}_0$ distributes a portion of a quantum state amongst external nodes $\mathcal{N}_1, \ldots, \mathcal{N}_k$ (in this illustration $k = 4$). This distribution is done through quantum channels, and thus may be vulnerable to a malicious eavesdropper, whose (potential) interaction is depicted with a red ring. To ensure a sense of security, the trusted nodes can adopt the trap code since the decryption operations are all performed locally.

connected to external nodes $\mathcal{N}_1, \ldots, \mathcal{N}_k$ via quantum channels, which may be simultaneously intercepted by a malicious adversary. The central node sends a portion of an entangled quantum state to each of the external nodes, after which the external nodes encode a local parameter on their portion of the quantum state for a spatially distributed quantum metrology scheme. The trap code can be adopted in this spatially distributed and multipartite framework since the decryption operations are local, and thus recover the same notions of privacy and soundness.

6.5 Quantum Metrology With Delegated Tasks

In the previous section, together the honest parties, Alice and Bob, had all of necessary quantum technologies to fully carry out a quantum metrology problem. In reality, fully implementing a quantum metrology problem is technologically demanding. Entangled quantum states must be generated and measured with high fidelity. The quantum internet [WEH18], and other asymmetric quantum networks, is a possible solution where parties which lack the necessary hardware can delegate the desired task to another party in the network. Of course, when delegating tasks, it is important to be mindful of possible risks. Within the framework of quantum

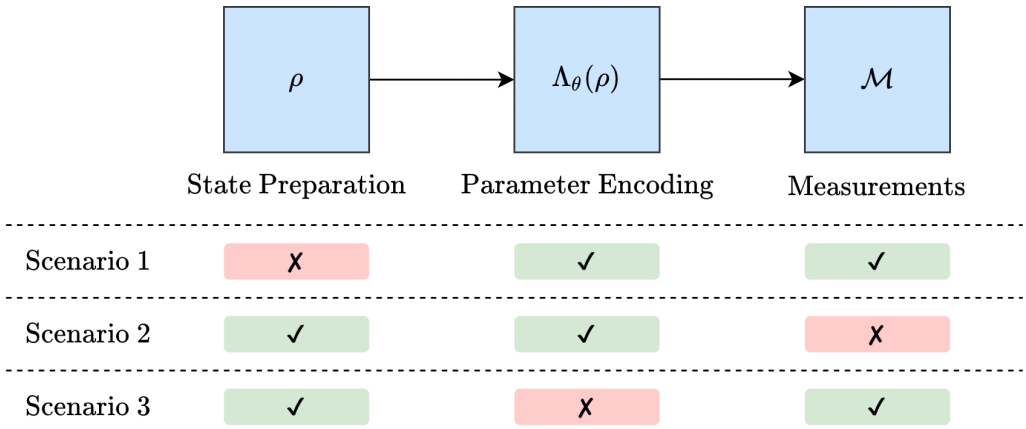


Figure 6.5: The different delegated quantum metrology scenarios addressed in the section. A quantum metrology problem can be decomposed into three (quantum) tasks: state preparation, parameter encoding and measurements. A red rectangle with a '✗' indicates that the task is delegated to a third party, as opposed to a green rectangle with a '✓' which indicates that the task is not delegated. In *scenario 1*, state preparation is delegated and verification protocols [ZH19a; MK20] are used to achieve a sense of security. In *scenario 2*, the measurements are delegated and we devise an authentication based protocol to achieve a sense of security. Finally, in *scenario 3*, the parameter encoding is delegated, and we discuss the impossibility of constructing a computationally secure protocol for such a scenario.

metrology, a malicious third party could bias the estimation results or conduct the estimate themselves. In this section, which is based off of work currently in preparation [SM], we propose cryptographic protocols to allow for delegating a portion of the quantum metrology scheme to an untrusted third party. This is done by partitioning a quantum metrology problem into three tasks: state preparation, parameter encoding and measurements, and explore the repercussions when a specific task, or a combination, is delegated. The different scenarios are summarized in Fig. (6.5). There is an additional task of processing the measurement results and creating the estimate, however we ignore this since it is inherently a classical computation.

6.5.1 Delegated State Preparation

The first scenario explored is when the task of quantum state preparation is delegated to an untrusted party. In the absence of a proper cryptographic protocol, the untrusted party could distribute any quantum state ρ', which could be preemptively biased to mask the true result of the parameter estimation. Because the metrology

portion part of the problem has not yet come into effect, we can utilize one of the many existing quantum state verification protocols [TM18; PLM18; MK20; Liu+19; Tak+19a], which ensure that the quantum state prepared is the desired quantum state.

Verification protocols are used to (as the name suggests) verify quantum states [ZH19a; ZH19b]. Typically, this is done by requesting additional copies of the desired quantum state and by measuring the additional copies in specific bases. The measurement results are used to decide if the protocol is accepted or rejected. It should be noted that most verification protocols are tailored for specific classes of quantum states, such as graph states [MK20; Tak+19a] or Dicke states [Liu+19]. More general protocols tend to require significantly more resources to achieve the same level of soundness for arbitrary quantum states [TM18; PLM18].

Of course, the soundness is dependent on the protocol chosen to be integrated into the cryptographic quantum metrology framework. For the sake of an example, consider the protocol outlined in [MK20]. The protocol is a verification protocol for graph states (and can thus be used for the bundled graph states introduced in **Chapter 4**), but naturally extends to all stabilizer states, including the GHZ state. The protocol takes advantage of the deterministic measurement results when a stabilizer state is measured in a basis of any of its stabilizers, Eq. (4.2). In summary, the protocol requests N copies of the desired stabilizer state, all but one (randomly selected) is measured with respect to an arbitrary stabilizer. The result is accepted if the $N-1$ measurements results all witness a $+1$ eigenvalue of their respective stabilizer. The protocol achieves a soundness of $\delta = 1/N$. Therefore, the integrity of the underlying quantum metrology problem is maintained if

$$N \geq \frac{\nu}{\alpha}. \tag{6.28}$$

After ν repetitions of the protocol, this translates to a quadratic increase in resources compared to the ideal framework.

Quantum state verification uses several figures of merit (besides just soundness) which are intertwined [ZH19a; ZH19b]. Specifically, the soundness is bounded for a fixed N, however the characterisation introduced in [ZH19a] permits the optimization of N for a fixed δ and α. For qubit stabilizer states the answer is $N = 2(\ln 2)^{-1}\delta^{-1}\ln\alpha^{-1}$. The bounds are different because the 'worst case' attack which saturates the soundness for a fixed N is different than the 'worst case' attack for a fixed δ.

6.5.2 Delegated Measurements

The second scenario we explore is the when the measurements are delegated to an untrusted third party. A simplistic version of this scenario with an honest-but-curious adversary has been explored [Tak+19b; Oka+20; Yin+20], where the authors propose using a blind quantum computing protocol [BFK09] to achieve privacy by masking the measurement results from an eavesdropper. However, blind quantum computing is not sufficient to achieve unconditional security, where no assumptions are made with respect to the adversary. For all intents and purposes, the untrusted party may return arbitrary measurement results, and without proper cryptographic precautions, the untrusted party can bias the estimate to their own accord. To combat this, the protocol we propose takes inspiration from verified blind quantum computing [Mor14; FK17] and the protocol proposed for quantum metrology over an unsecured quantum channel.

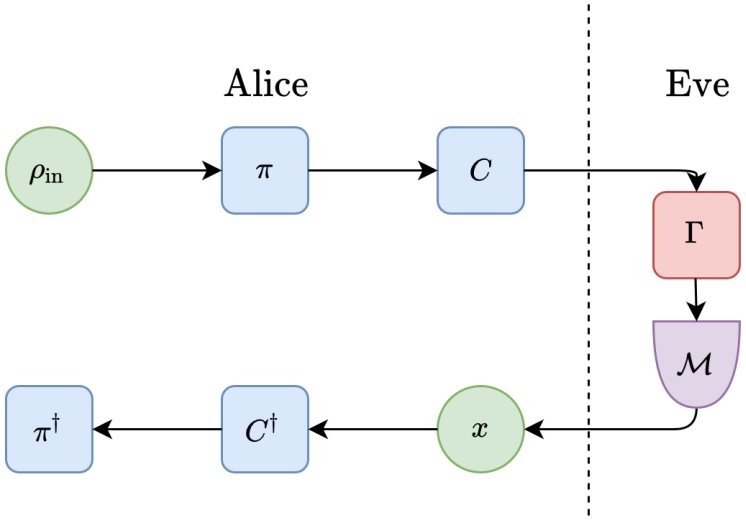


Figure 6.6: Alice prepares the quantum state ρ_{in}, which is a combination of an n for quantum metrology and t flag qubits. Before sending the quantum state to Eve, Alice randomly permutes the flag qubits amongst the encoded qubits and subsequently encrypts the quantum state by applying a random Pauli C. Without loss of generality, the measurement result, x, returned by Eve will coincide with the measurement statistics of $\mathcal{M}\big(\Gamma(C\pi\rho_{\text{in}}\pi^\dagger C^\dagger)\big)$, where Γ is any CPTP map. Upon receipt, Alice performs classical post-processing on x such that it can be properly interpreted. This is represented as applying $C^\dagger$ and $\pi^\dagger$ on $\mathcal{M}\big(\Gamma(C\pi\rho_{\text{in}}\pi^\dagger C^\dagger)\big)$.

Using the same nomenclature as the protocol for quantum metrology over an unsecured quantum network: Alice is the trusted party who lacks the necessary quantum hardware to execute quantum measurements, and Eve is the untrusted

party who is delegated the measurements task. In a trusted setting, Alice sends Eve an encoded quantum state ρ_θ, and the probability of Eve returning a specific measurement result corresponds to the amplitudes of $\mathcal{M}(\rho_\theta)$. In the untrusted setting, Eve can return arbitrary measurement results, but without loss of generality, they will correspond to the amplitudes of $\mathcal{M}(\rho'_\theta)$, where ρ'_θ is an arbitrary and not necessarily encoded quantum state. In addition, Eve can perform the correct measurement, such that they can construct an estimate of θ for themselves and send a biased or nonsensical results back to Alice. To attain a notion of security and privacy, Alice employs the protocol illustrated in Fig. (6.6) and described below.

The protocol we outline is specific to the case when, in the ideal framework, Alice would request Eve to measure each qubit respect to the basis of a (non-identity) Pauli operator P. It can be adapted to other non-entangled measurements by appropriately rotating the encryption operations. We focus on simple measurements as the protocol is more tangible: it only requires local Clifford operations to encrypt the quantum state. It is also practical as feasible measurement strategies in quantum metrology are typically with respect to the eigenbasis of a Pauli operator because they are the simplest to implement.

Implementation Instructions:

1. Alice prepares the $m = n + t$ qubit state $\rho_{\text{in}} = \rho_\theta \otimes |0\rangle\langle 0|^{\otimes t}$. Here, ρ_θ is the n qubit encoded quantum state and $|0\rangle\langle 0|^{\otimes t}$ is used ancillary flag qubits as ancillary flag qubits because of their deterministic measurement outcome.

2. Alice encrypts ρ_{in} by first performing a permutation π and then applies a random Clifford $C \in \mathcal{C}_1^{\otimes m}$. The permutation will insert the flag qubits at random positions so that Eve cannot distinguish between the encoded qubits and flag.

3. Alice requests Eve to measure the quantum state in the basis of $C\pi P^{\otimes n} \otimes Z^{\otimes t}\pi^\dagger C^\dagger$, the measurement is represented by the map $\mathcal{M}$.

4. Eve returns a measurement result x, which are derived from the measurement statistics $\mathcal{M}\big(\Gamma(C\pi\rho_{\text{in}}\pi^\dagger C^\dagger)\big)$, where Γ is any CPTP map.

5. Alice performs classical post-processing on m to obtain the measurement result as if it had not been encrypted. With respect to the measurement statistics, this is represented by applying $\pi^\dagger C^\dagger$ to $\mathcal{M}\big(\Gamma(C\pi\rho_{\text{in}}\pi^\dagger C^\dagger)\big)$.

6. Alice accepts the measurement result if, after post-processing, the measurement results of the t flag qubits coincide with the expected result of $|0\rangle\langle 0|^{\otimes t}$. Otherwise, Alice rejects the measurement results as Eve must have acted maliciously.

The reason the protocol is designed[3] for measuring with respect to an eigenbasis of a Pauli operator $P^{\otimes n}$, is because regardless of the encryption C, the requested measurement is an random string of Pauli operators, and Eve cannot decipher which measurements coincide with qubits for quantum metrology and which measurement results coincide with ancillary flag qubits. As a result, the protocol is completely private

$$\mathbb{E}(\rho_E) = \mathbb{I}/2^m, \tag{6.29}$$

where the above privacy statement can be shown using the same logic as the privacy of the trap code for quantum metrology over an unsecured quantum channel, Eq. (6.27).

In **Appendix C**, we show that the soundness of this protocol is bounded below the soundness of the trap code for quantum metrology over an unsecured quantum channel, and thus $\delta = \frac{3n}{2t}$. Therefore, the integrity of the underlying quantum metrology problem is maintained if $\frac{3n}{2\alpha t} \leq \nu^{-1}$. Equivalently, the number of ancillary flag qubits required is $t \geq \frac{3n\nu}{2\alpha}$. Thus, the cryptographic framework requires a quadratic increase in the number of resources to maintain the same level of precision as the ideal framework.

6.5.3 Delegated Parameter Encoding

The final scenario considered is when the task of parameter encoding is delegated to an untrusted third party. From a verification perspective, the goal is to assure that some output state ρ_{out} is close to the ideal encoded state ρ_θ with high probability. Unsurprisingly, this is an impossible task from an information theoretic standpoint without having perfect knowledge of θ, which would entirely defeat the purpose of quantum metrology. The impossibility of this task stems from the fact that an adversary can manipulate the lack of information about θ to their advantage. For example, an adversary can introduce a slight bias $\Lambda_{\theta+\delta\theta}$, encode a different parameter altogether Λ_φ, encode θ into a different quantum state $\tilde{\rho}$, or do nothing at all $\mathbb{I}$.

[3] To adapt the protocol to more complex measurements, the encryption on the requested measurement basis would have to mimic the actions of an arbitrary Clifford operation on a Pauli operator.

Furthermore, there is no way of guaranteeing that an adversary acts identically each round.

Suppose that the information theoretic standpoint is abandoned and the abilities of the adversary are greatly limited to either applying Λ_θ or the identity $\mathbb{I}$. If one has a priori knowledge that $\theta \approx \theta_0$, a loose 'accept' criteria is for the estimate to be within some range of θ_0. This 'protocol' can still be manipulated by an adversary if they learn the range of acceptance: $\mathbb{I}$ is applied a small number of times such that the expected estimate falls within the acceptance range despite the added bias.

Finally, if the adversary is further hindered by assuming that they cannot access any sort of classical information - such as an a priori approximation $\theta \approx \theta_0$, or the acceptance range of the aforementioned protocol - then one can continue on with the quantum metrology scheme. This is because in this specific setting, the effective encoding map is now the CPTP map

$$\rho \to (1-p)\Lambda_\theta(\rho) + p\rho, \tag{6.30}$$

where p is the effective probability that the adversary does nothing, and hence applies Λ_θ with effective probability $1-p$. Here, the metrology problem of estimating θ has evolved into the multiparameter problem [RJD16] of estimating θ and p. However, in making these assumptions, we have ventured out of the realm of cryptographic quantum metrology and into a fusion of quantum channel tomography [BPP08] and quantum metrology.

6.6 Discussion

The work presented in this chapter is a novel approach to immerse a general quantum metrology problem in a cryptographic framework. By demanding the final measurement statistics used to construct an estimate are close to that of the ideal framework (sans malicious adversary), the cryptographic notion of soundness can be related to the integrity of the quantum metrology problem. Within the frequentist approach, in an ideal framework, the estimate converges to the true value as $\nu \to \infty$, so any added uncertainty as a result of the cryptographic framework, ε, will be the factor which limits the precision in the cryptographic framework. The 'cryptographic uncertainty' was presented as a result of the interference of a (potentially) malicious adversary, but in reality, the integrity statements hold for any resource satisfying Eq, (6.8). For example, the uncertainty caused by faulty quantum hardware or

environmental noise.

The soundness of the protocols are derived for unconditional security, i.e no assumptions about the adversary are made. Of course, by discarding this assumption and limiting the abilities of an adversary (for example, only local Clifford operations, etc), the soundness bounds can be greatly improved, thus reducing the number of ancillary flag qubits to maintain the functionality of the underlying quantum metrology. Additionally, the protocols are designed for qubit systems, which naturally generalize to qudit systems, however, the protocols do not easily translate to a continuous variable quantum system; properly deriving the analogous results is a future perspective of this work.

From a cryptographic standpoint, there are numerous ways to broaden the perspective of quantum metrology in a cryptographic framework. For example, the untrusted parties in the delegated task framework can be replaced by untrusted devices to attain a notion of device independent [MY98; Xu+14] quantum metrology. Alternatively, the notions of cryptography introduced can be further abstracted [MR11] to attain a notion of quantum metrology in an abstract cryptographic framework.

At first glance of the integrity statements throughout this chapter, the statistical significance α may seem like an undesirable quantity and counter-intuitive to the unconditional security assumptions. However, a bound on the trace distance cannot be made in any other way. Consider the problem of performing quantum metrology over an unsecured quantum channel, if a malicious party replaces the quantum state by the maximally mixed state, then (regardless of the protocol) the measurement results of the 'flag qubits' will result in accept with a very small but non-zero probability. In this example, the quantum state then used for quantum metrology would be useless. Formally, the statistical significance parameter α used throughout quantum authentication and verification [ZH19a; ZH19b] is identical to the notion of confidence level $1 - \alpha$ used in traditional statistics. In which, α is a pre-decided upon value related to the probability of rejecting the null-hypothesis, or in this case the outcome of the protocol.

The two protocols presented for quantum metrology over an unsecured quantum channel differ in practicability and efficiency. Although the Clifford code is more efficient, the required entanglement is highly impractical. In contrast the trap code is only slightly more demanding than non-secure versions, requiring only local Clifford operations for encryption. For the task of delegated measurements, we designed a protocol analogous to the trap code. We could have additionally made an analogous protocol to the Clifford code for the same task, however this would require Alice requesting highly entangled measurements to be performed, which seems more out

of reach than a highly entangled unitary operation. These protocols can also be made somewhat robust to noise by tweaking acceptance parameters [UM20].

In Fig. (6.5), three scenarios for quantum metrology with delegated tasks are presented. Separately, we show that the task of state preparation and measurements can be delegated to an untrusted third party if reinforced with a proper cryptographic protocol. The natural question to ponder is if both tasks can be delegated to a third party, where the trusted party, Alice, can only perform the encoding map Λ_θ and a set of encryption operations. At first glance, this seems possible by fusing the verification protocol of [MK20] and the protocol presented for delegated measurements. A local Clifford encryption guarantees absolute privacy and soundness is easily derived for the case when $\Lambda_\theta = \mathbb{I}$. As the nature of Λ_θ should have little to no impact on the soundness, it ought to follow that a similar derivation can be performed for any CPTP encoding Λ_θ. A future perspective is to prove and verify this claim.

7 Remarks

La volonté trouve, la liberté choisit. Trouver et choisir, c'est penser.

-Victor Hugo

Quantum metrology is a promising discipline of quantum information; it has a broad scope of applications in a variety of scientific fields and is currently witnessing an abundance experimental and theoretical developments. The objective of quantum metrology is to use quantum probes to estimate unknown parameters as accurately as possible. By capitalizing on quantum properties, it is possible to achieve a precision which is unobtainable using the best classical strategies. This thesis explored how other quantum techniques can be appropriately incorporated within the realm of quantum metrology. Specifically, the utility of graph states, the limitations of quantum error correction, and the consequences of a cryptographic framework. Within each scenario, the idealized 'Heisenberg limit precision' is used as a figure of merit.

The work in this thesis is uniquely theoretical, even so, the general philosophy was to be relevant and applicable to the first generations of quantum hardware. Graph states can be constructed using only control-Z operations and the QFI of graph states can be approximately saturated using single qubit measurements (**Chapter 4**). The error correction protocol in **Chapter 5** is currently realizable [Dut+07; Tam+14; Wal+14]. Most of the cryptographic protocols presented in **Chapter 6** use local encryption/decryption operations and use local measurements on ancillary qubits. One concern may be that the noise models are 'too idealized' and the adversarial tools are 'too abstract', and in general these will be dependent on the quantum hardware. In reply, the models presented in this thesis are a baseline and can be straightforwardly adapted to better describe the desired setting -

as any experimental setup will be extremely dependent on the implementation and the available technologies.

Another general philosophy we strove to maintain was a sense of generality from the perspective of quantum metrology. However, an arbitrary parameter encoding map Λ_θ is quite vague and the equations pertaining to parameter estimation are highly non-linear, making it difficult to draw conclusions from the most general situation. Instead, we often used the frequentist approach to phase estimation as a baseline example. This example, is canonical with quantum metrology and has several applications [HB93; Par09; GLM11]. Nonetheless, many of the mathematical tools and derivations can be adapted to specific Λ_θ. In particular with respect to **Chapter 4**, if $\Lambda_\theta = e^{-i\theta G}$, then the QFI can be defined as a relationship between the stabilizer group of the initialized quantum state and the expansion of G and G^2. As hypothesized in **Chapter 5**, similar results for the limitations of error correction are likely obtained regardless of Λ_θ, note that it is necessary to implement an error correction protocol that does not interfere with Λ_θ.

Similarly, most of the mathematical tools and results can be adapted to the multiparameter quantum metrology. The main difficulty, incompatibility of simultaneous measurements [RJD16], is a standard across the multiparameter framework and not inherent to any of the settings we explored. Although not explicitly proven, if there does exists a set of compatible measurements, then the integrity of the estimate for each parameter in a cryptographic framework will be of the form Eq. (6.14) and Eq. (6.17). The reason being that an equivalent derivation would follow from a secondary (compatible) measurement (and all subsequent measurements) because of the definition of the trace distance. A future perspective is to formally address this question.

Aside from the brief summary of Bayesian statistical interference in **Chapter 3**, this thesis is void of the Bayesian approach to quantum metrology [Hol82; JD15; RKD18]. Because the work of **Chapter 4** is heavily influenced by the QFI, which is not used in the Bayesian approach, it is unclear if the shape of a graph can be related to the practicality of the corresponding graph state for phase estimation using a Bayesian approach. With respect to **Chapter 6**, it is impossible to gauge the integrity of a Bayesian quantum metrology problem within a cryptographic framework without first specifying a cost function, Eq. (3.23), and estimation strategy.

7.1 Summary Of Results And Future Perspectives

7.1.1 Chapter 4

In **Chapter 4**, we demonstrate that graph states - in conjunction with their existing versatility - are a useful resource for quantum metrology. This is done by constructing a class of graph states, named bundled graph states, which possess a large amount of internal symmetry, and in consequence can approximately saturate the Heisenberg limit. More so, graph states are robust against dephasing noise and a small number of erasures, and the QFI can be approximately saturated with a simple measurement scheme. The robustness against a small number of erasures is compelling as the standard resource for phase estimation, GHZ states, lose all functionality after a single erasure [TA14].

By construction, bundled graph states are a natural resource for multiparameter metrology, specifically in the context of quantum sensing networks [Kóm+14; Eld+18; PKD18; Rub+20]. Each bundle can be subjected to independent parameter encoding schemes. The robustness derivations can be generalized for noise models which are bundle dependent, and a compatible measurement scheme arises from the fact that not all parameters are encoded into each qubit.

7.1.2 Chapter 5

The limitations of error correction enhanced quantum metrology is outlined in **Chapter 5**. In contrast to previous results, which state that the Heisenberg limit can be permanently achieved if the signal and noise are orthogonal [DCS17; Zho+18], we show that when hardware limitations are accounted for, the Heisenberg limit is eventually lost. As expected, if the frequency of error correction is high enough, the Heisenberg limit is achieved for a serviceable duration of time. Even though the focus is a single error correction protocol, we conjecture that the results translate to any error correction protocol or noise mitigation strategy, as small deviations of the phase caused by noise cannot be perfectly corrected. Eventually these small deviations accumulate enough such that the quantum state is useless for quantum metrology.

7.1.3 Chapter 6

In the presence of a (potential) malicious adversary, many notions of estimation theory have to be altered in some capacity. This is simply because there is no guarantee of having access to the ideal resource, leading to ambiguity in the construction of an estimator. In **Chapter 6**, we formalize the consequences of quantum metrology within a cryptographic framework. The idea is to use the same estimation strategy as if there was no malicious adversary, and if an appropriate protocol is used to detect any malicious alterations, then the soundness of said protocol can be linked to the integrity of the quantum metrology problem. Integrity is a concept used in quantum cryptography, which quantifies the ability to retain the functionality of the underlying process, in this case the underlying process is quantum metrology, and so we decided that the integrity will encapsulate any added bias and the difference in precision.

Additionally, in **Chapter 6**, we constructed several cryptographic protocols for cryptographic quantum metrology. The cryptographic protocols are each motivated by the absence of the necessary quantum hardware to fully execute the quantum metrology task, forcing interactions with a third party. For example, protocols to transmit quantum information across an unsecured quantum channel, and protocols to guarantee security when a task, either quantum state verification or quantum measurements, are performed by an untrusted party. It goes without saying that it is impossible to delegate the task of parameter encoding to an untrusted party, as this defeats the purpose of quantum metrology.

The immersion of quantum cryptography into quantum metrology is a novel area of research, and as such there are several future perspectives. Just as the first generations of quantum technologies will be limited in abilities, so too will be the abilities of a malicious adversary. In our work, in order to fulfill a notion of computational security, no assumptions about the malicious adversaries are made. By limiting the possible attacks a malicious adversary can perform (as one expects), an improved notion of cryptographic soundness is achieved. One concern of the quantum cryptography protocols presented in **Chapter 6** is the dependence on noiseless quantum operations, this restriction can be loosened by tweaking acceptance parameters [UM20]. Lastly, a possible future research direction is to consider continuous variable resources, because it is not obvious if the analogous protocols will satisfy the same soundness inequalities.

7.2 Secure Sensing Networks

An ongoing project of mine is to adopt quantum sensing networks [Kóm+14; Eld+18; Ge+18; PKD18; ZZS18; Rub+20; Guo+20] into the realm of quantum metrology in a cryptographic framework. This is a logical next step in the direction of cryptography and quantum metrology, as there exists a plethora of secure multipartite protocols across quantum networks [Pap+12; Hua+19] and the foundation introduced in **Chapter 6** is easily adapted to the network setting. Additionally, the authors of [Kóm+14], who proposed a clock synchronization scheme across a quantum network, are the first to consider the security aspect of a quantum metrology problem.

The idea is straightforward: there is a central node who has the ability to prepare highly entangled quantum states, qubits are then distributed throughout the network for a multiparameter quantum metrology problem. We introduce two types of malicious adversaries: the first are eavesdroppers who can interact with the quantum channels, and the second are some of the exterior nodes of the network who may behave maliciously. By adapting the protocols introduced in [SMK21; SM] to the network setting, we establish the concept of a secure quantum sensing network.

In addition to the cryptographic notions of soundness, privacy and integrity, the notion of anonymity is introduced to quantum sensing networks [Unn+19]. We define anonymity within quantum sensing networks to mean that the local parameters cannot be estimated from the measurement results, only a global parameter, for example, an average of the parameters. For example, the total power consumption of all appliances may be transmitted to a power supplier, but not the consumption of individual appliances. In some sense, anonymity is a form of privacy.

Somewhere, something incredible is waiting to be known.

-Carl Sagan

A
Robustness of Graph States Subjected to Noise

Recall that a graph $G = (V, E)$ is divided into disjoint subsets $U_1, U_2, \ldots, U_l, \ldots$ such that $\bigcup_l U_l = V$. The vertices are partitioned in accordance to commonly shared neighbourhoods, hence, if $v_i \in U_a$ and $v_j \in U_b$, then $N(v_i) = N(v_j)$ if $a = b$ and $N(v_i) \neq N(v_j)$ if $a \neq b$. We write that $|U_l| = u_l$ and the shared neighbourhood of U_l is M_l with $|M_l| = m_l$.

In both proofs, sums are taken over all possible combinations of qubits, indexed by vectors. When these vectors are summed, it is taken modulo 2. For example if $\vec{j} = \{1, 1, 0\}$ and $\vec{k} = \{1, 0, 1\}$, then $\vec{j} + \vec{k} = \{0, 1, 1\}$.

A.1 Robustness Against IID Dephasing

After a graph state undergoes iid dephasing, it can be expressed as

$$\sum_{\vec{j}} p^j (1-p)^{n-j} Z_{\vec{j}} \left|G\right\rangle\!\left\langle G\right| Z_{\vec{j}}. \tag{A.1}$$

Conveniently, the above quantum state is already expressed as a sum of orthogonal pure states, computing the QFI is then a straightforward use of the general expression

$$\mathcal{Q}(G^{\text{dephasing}}) = \frac{1}{2} \sum_{\vec{j},\vec{k}} \frac{(\lambda_{\vec{j}} - \lambda_{\vec{k}})^2}{\lambda_{\vec{j}} + \lambda_{\vec{k}}} \left| \left\langle G\right| Z_{\vec{j}} \sum_i X_i Z_{\vec{k}} \left|G\right\rangle \right|^2, \tag{A.2}$$

where $\lambda_{\vec{j}} = \lambda_j = p^j(1-p)^{n-j}$. The only non-vanishing terms in the sum occurs when $\vec{j} + \vec{k} = M_l$ for some l. We divide $\vec{k}$ into three disjoint parts, a qubits with a flipped phase from the set U_l, b qubits with a flipped phase from M_l, and c qubits from the remaining qubits

$$\begin{aligned}\mathcal{Q}(G^{\text{dephasing}}) &= \frac{1}{2}\sum_l \sum_{\vec{k}} \frac{(\lambda_{\vec{k}+M_l} - \lambda_{\vec{k}})^2}{\lambda_{\vec{k}+M_l} + \lambda_{\vec{k}}} \left| \langle G| Z_{\vec{k}+M_l} \sum_i X_i Z_{\vec{k}} |G\rangle \right|^2 \\ &= \frac{1}{2}\sum_l \sum_{a=0}^{u_l} \sum_{b=0}^{m_l} \sum_{c=0}^{n-u_l-m_l} \frac{(\lambda_{a-b+c+m_l} - \lambda_{a+b+c})^2}{\lambda_{a-b+c+m_l} + \lambda_{a+b+c}} (u_l - 2a)^2 \\ &= \sum_l f_l g_l,\end{aligned} \tag{A.3}$$

where

$$f_l = u_l^2(1-2p)^2 + 4u_l p(1-p) \geq u_l^2(1-2p)^2, \tag{A.4}$$

and

$$\begin{aligned} g_h &= \frac{1}{2}\sum_{j=0}^{m_l} \binom{m_l}{j} \frac{\left(p^{m_l-j}(1-p)^j - p^j(1-p)^{m_l-j}\right)^2}{p^{m_l-j}(1-p)^j + p^j(1-p)^{m_l-j}} \\ &\geq 1 - \left(2p(1-p) + 1/2\right)^{m_l} \\ &\geq 1 - \left(2p(1-p) + 1/2\right)^{m}, \end{aligned} \tag{A.5}$$

where $m = \min_l m_l$. Combining the bounds of f_l and g_l with the fact that $\sum_l u_l^2 = \mathcal{Q}(G)$, one obtains

$$\mathcal{Q}(G^{\text{dephasing}}) \geq (1-2p)^2 \Big(1 - \left(2p(1-p) + 1/2\right)^m\Big) \mathcal{Q}(G). \tag{A.6}$$

A.2 Robustness Against Finite Erasures

We return to the stabilizer representation to obtain a useful closed form expression for a graph state $\vec{G}$ subjected to erasures indexed by $\vec{e}$

$$|G\rangle \to \text{Tr}_{\vec{e}} |G\rangle\langle G| = \frac{1}{2^n} \sum_{S \in \mathcal{S}} \text{Tr}_{\vec{e}}\, S. \tag{A.7}$$

Recall that the stabilizer group $\mathcal{S}$ can be generated by generators $g_i = X_i \bigotimes_{j\in N(i)} Z_j$. Therefore each stabilizer S can be written in the form

$$S = g_1^{a_1} g_2^{a_2} \dots g_n^{a_n}, \tag{A.8}$$

where $a_j \in \{0, 1\}$. Thus, $\mathrm{Tr}_{\vec{e}}\, S$ vanishes under two conditions. The first is if $a_x = 1$ for any x indexed by $\vec{e}$. The second is if $\sum_{j\in N(x)} a_j \equiv 1 \mod 2$ for any x indexed $\vec{e}$. Define the set $L_{\vec{e}}$ to be set of erased qubits and their neighbourhoods

$$L_{\vec{e}} = \bigcup_{x\in\vec{e}} \{x\} \cup N(x). \tag{A.9}$$

Define $\tilde{Z}$ to be the set of all possible combination of Z operators indexed by a subset of $L_{\vec{e}}$

$$\tilde{Z} = \{Z_{\vec{j}} \mid \vec{j} \subseteq L_{\vec{e}}\}. \tag{A.10}$$

Any stabilizer S which is traced out, i.e $\mathrm{Tr}_{\vec{e}}\, S = 0$, will commute with half of Pauli operators in $\tilde{Z}$ and anti-commute with the other half. Any stabilizer which is not traced out will commute with all of the operators. From which it follows that, the quantum state after going erasures indexed by $\vec{e}$ can be expressed as

$$2^{-|L_{\vec{e}}|} \sum_{\vec{j}\in L_{\vec{e}}} Z_{\vec{j}} \,|G\rangle\langle G|\, Z_{\vec{j}}. \tag{A.11}$$

As it was noted in the main text, the above mixed state is left as n qubit state for clarity. The traced out systems are equivalent to maximally mixed states, $\mathbb{I}/2$, which are irrelevant with respect to the QFI.

The quantum state in Eq. (A.11) is written as a sum of orthonormal pure states. The QFI is thus

$$\begin{aligned} \mathcal{Q}(G^{\text{erasures } \vec{e}}) &= \frac{1}{2} \sum_{\vec{j},\vec{k}} \frac{(\lambda_{\vec{j}} - \lambda_{\vec{k}})^2}{\lambda_{\vec{j}} + \lambda_{\vec{k}}} \big| \langle G| Z_{\vec{j}} \sum_i X_i Z_{\vec{k}} |G\rangle \big|^2 \\ &= \frac{1}{2} \sum_l \sum_{\vec{k}} \frac{(\lambda_{\vec{k}+M_l} - \lambda_{\vec{k}})^2}{\lambda_{\vec{k}+M_l} + \lambda_{\vec{k}}} \big| \langle G| Z_{\vec{k}+M_l} \sum_i X_i Z_{\vec{k}} |G\rangle \big|^2, \end{aligned} \tag{A.12}$$

where $2^{-|L_{\vec{e}}|}$ if $\vec{j} \subseteq L_{\vec{e}}$ and 0 otherwise. It follows then that $\lambda_{\vec{k}+M_l} - \lambda_{\vec{k}} = 0$ if $\vec{k}, \vec{k} + M_l \subseteq L_{\vec{e}}$. Regardless of $\vec{k}$, this only occurs if $M_l \subseteq L_{\vec{e}}$. If $M_l \nsubseteq L_{\vec{e}}$, the sum

over $\vec{k}$ depends on if $U_l \subseteq L_{\vec{e}}$ or $U_l \nsubseteq L_{\vec{e}}$

$$\mathcal{Q}(G^{\text{erasures } \vec{e}}) = \sum_l h_l(\vec{e}), \tag{A.13}$$

where

$$h_l(\vec{e}) = \begin{cases} u_l^2 & \text{if } M_l \nsubseteq L_{\vec{e}} \text{ and } U_l \nsubseteq L_{\vec{e}} \\ u_l & \text{if } M_l \nsubseteq L_{\vec{e}} \text{ and } U_l \subseteq L_{\vec{e}}\,. \\ 0 & \text{otherwise} \end{cases} \tag{A.14}$$

B

QFI of a Noisy GHZ State

B.1 Solving The Master Equation

The dynamics of **Chapter 5** are governed by the master equation

$$\frac{d\rho}{dt} = -\frac{i}{\hbar}[H, \rho] + \gamma \sum_{m=1}^{n} (X_m \rho X_m - \rho), \tag{B.1}$$

with $H = \frac{\hbar\omega}{2} \sum_{m=1}^{n} Z_m$. In this appendix, we derive the solutions to the dynamics, as well as the modified version in which error correction is incorporated. Without loss of generality, it can be assumed that the solution is of the form

$$\rho = \sum_{j,k} \alpha_{j,k} \left|j\right\rangle\!\left\langle k\right|, \tag{B.2}$$

where $j, k \in \{0, 1\}^{\otimes n}$ are bit strings of length n. As such, one approach to solving the master equation, Eq. (B.1), is to view it a system of linear differential equations with respect to the amplitudes $\alpha_{j,k}$. Because, the quantum state is initialized in a GHZ state, the only non-zero amplitudes are those of the form $\alpha_{j,j}$ or $\alpha_{j,\bar{j}}$, where $|\bar{j}\rangle = X^{\otimes n} |j\rangle$. Furthermore, the system of differential equation can be divided into two independent equations

$$\frac{d\vec{a}}{dt} = A\vec{a}, \tag{B.3}$$

$$\frac{d\vec{b}}{dt} = B\vec{b}, \tag{B.4}$$

where $\vec{a}$ ($\vec{b}$) is a vector of size 2^n containing all of the amplitudes of the form $\alpha_{j,j}$ ($\alpha_{j,\bar{j}}$), and

$$A = \sum_{m=0}^{n-1} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^{\otimes m} \otimes \begin{pmatrix} -\gamma & \gamma \\ \gamma & -\gamma \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^{\otimes n-m-1}, \tag{B.5}$$

$$B = \sum_{m=0}^{n-1} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^{\otimes m} \otimes \begin{pmatrix} -i\omega - \gamma & \gamma \\ \gamma & i\omega - \gamma \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^{\otimes n-m-1}. \tag{B.6}$$

Both and A and B are time-independent, therefore the solutions are given by the corresponding matrix exponential: $\vec{a} = e^{At}\vec{a}_0$ and $\vec{b} = e^{Bt}\vec{b}_0$ (here $\vec{a}_0$ and $\vec{b}_0$ are the initial amplitude vectors), where

$$e^{At} = e^{-n\gamma t} \begin{pmatrix} \cosh(\gamma t) & \sinh(\gamma t) \\ \sinh(\gamma t) & \cosh(\gamma t) \end{pmatrix}^{\otimes n} = e^{-n\gamma t} \begin{pmatrix} c_\gamma & s_\gamma \\ s_\gamma & c_\gamma \end{pmatrix}^{\otimes n}, \tag{B.7}$$

and

$$e^{Bt} = e^{-n\gamma t} \begin{pmatrix} \cos(\Delta t) - i\frac{\omega}{\Delta}\sin(\Delta t) & \frac{\gamma}{\Delta}\sin(\Delta t) \\ \frac{\gamma}{\Delta}\sin(\Delta t) & \cos(\Delta t) + i\frac{\omega}{\Delta}\sin(\Delta t) \end{pmatrix}^{\otimes n} = e^{-n\gamma t} \begin{pmatrix} x_- & y \\ y & x_+ \end{pmatrix}^{\otimes n}, \tag{B.8}$$

with $\Delta = \sqrt{\omega^2 - \gamma^2}$. Because this is a solution with complex solutions, there are no issues when $\gamma^2 > \omega^2$, this maps the usual trigonometric functions (cos and sin) to their hyperbolic counterparts (cosh and sinh). The notation - $c_\gamma = \cosh(\gamma t)$, $s_\gamma = \sinh(\gamma t)$, $y = \frac{\gamma}{\Delta}\sin(\Delta t)$ and $x_\pm = \cos(\Delta t) \pm i\frac{\omega}{\Delta}\sin(\Delta t)$ - is used for conciseness.

B.2 QFI Without Error Correction

In the case without error correction, one can simply use the solutions of the differential equations, Eq. (B.7) and Eq. (B.8). The quantum state at time t is given by

$$\rho = \frac{1}{2}\sum_j \lambda_{j,+} |\psi_{j,+}\rangle\langle\psi_{j,+}| + \lambda_{j,-} |\psi_{j,-}\rangle\langle\psi_{j,-}|, \tag{B.9}$$

with

$$\lambda_{j,\pm} = e^{-n\gamma t}\frac{s_j \pm r_j}{2}, \tag{B.10}$$

and

$$|\psi_{j,\pm}\rangle = \frac{1}{\sqrt{2}}\big(e^{-i\theta_j/2}\,|j\rangle \pm e^{+i\theta_j/2}\,|\bar{j}\rangle\big). \tag{B.11}$$

The factor of $1/2$ in front of the sum is to avoid double counting, because $\lambda_{j,\pm} = \lambda_{\bar{j},\pm}$ and $|\psi_{j,\pm}\rangle = |\psi_{\bar{j},\pm}\rangle$. The eigenvalues and eigenvectors are parameterized by

$$s_j = c_\gamma^{n-h_j} s_\gamma^{h_j} + c_\gamma^{h_j} s_\gamma^{n-h_j}, \tag{B.12}$$

$$r_j e^{\pm i\theta_j} = x_\pm^{h_j} y^{n-h_j} + x_\mp^{n-h_j} y^{h_j}, \tag{B.13}$$

where h_j is the Hamming weight (number of 1's) of j. Using the general formula for the QFI, one obtains

$$\begin{aligned}
\mathcal{Q}_{\text{noisy}} &= \frac{1}{2}\sum_j \left(\frac{\dot{\lambda}_{j,+}^2}{\lambda_{j,+}} + \frac{\dot{\lambda}_{j,-}^2}{\lambda_{j,-}} + 2\frac{(\lambda_{j,+}-\lambda_{j,-})^2}{\lambda_{j,+}+\lambda_{j,-}} \Big(\big|\, \langle\psi_{j,+}|\dot{\psi}_{j,-}\rangle \,\big|^2 + \big|\, \langle\psi_{j,-}|\dot{\psi}_{j,+}\rangle \,\big|^2 \Big) \right) \\
&= \frac{e^{-n\gamma t}}{2}\sum_j \frac{s_j \dot{r}_j^2}{s_j^2 - r_j^2} + \frac{r_j^2}{s_j}\dot{\theta}_j^2 \\
&= n^2 t^2 \Big(1 - \big(2 - \frac{4}{3n}\big)\gamma t\Big) + \mathcal{O}\big(t^4\big),
\end{aligned} \tag{B.14}$$

where the notation $\dot{\square} = \partial_\omega \square$ for clarity and the factor of $1/2$ in front of the sum is again used to avoid double counting.

B.3 QFI Using The Parity Check Code

The overall dynamics are modified upon inclusion of error correction. The system evolves in accordance to the master equation, Eq. (B.1), for time τ, after which an error correction operation is performed. This process is repeated until the total time t has passed (it is assumed that t/τ is an integer).

To incorporate the parity check code into the dynamics, the evolution of the ancillary qubit (indexed by $m = n+1$), which is subjected to dephasing with a rate of ξ, must be tracked. The matrix solutions of this altered system are

$$e^{A\tau} = e^{-(n\gamma+\xi)\tau} \begin{pmatrix} c_\gamma & s_\gamma \\ s_\gamma & c_\gamma \end{pmatrix}^{\otimes n} \otimes \begin{pmatrix} c_\xi & s_\xi \\ s_\xi & c_\xi \end{pmatrix}, \tag{B.15}$$

and

$$e^{B\tau} = e^{-(n\gamma+\xi)\tau} \begin{pmatrix} x_- & y \\ y & x_+ \end{pmatrix}^{\otimes n} \otimes \begin{pmatrix} c_\xi & s_\xi \\ s_\xi & c_\xi \end{pmatrix}, \tag{B.16}$$

where $c_\xi = \cosh(\xi\tau)$ and $s_\xi = \sinh(\xi\tau)$. Note that the other variables - c_γ, s_γ, y and $x_\pm$ - are in terms of τ here (not t).

When using the parity check code, a correction is made on a sensing qubit if it has a different parity than the ancillary qubit. Imperfect syndrome diagnosis is simulated by adding a probability that the syndrome diagnosis outputs an incorrect result with probability p. The overall dynamics of the error correction can be translated into the matrix language

$$E = \begin{pmatrix} 1-p & 1-p \\ p & p \end{pmatrix}^{\otimes n} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} p & p \\ 1-p & 1-p \end{pmatrix}^{\otimes n} \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \tag{B.17}$$

Combing everything, the amplitudes after time t, and therefore t/τ applications of the parity check code, is

$$\begin{aligned} \vec{a} = \left(Ee^{A\tau}\right)^{t/\tau}\vec{a}_0 = e^{-\xi t}\Bigg(& \begin{pmatrix} 1-p & 1-p \\ p & p \end{pmatrix}^{\otimes n} \otimes \begin{pmatrix} c_\xi & s_\xi \\ 0 & 0 \end{pmatrix} \\ & + \begin{pmatrix} p & p \\ 1-p & 1-p \end{pmatrix}^{\otimes n} \otimes \begin{pmatrix} 0 & 0 \\ s_\xi & c_\xi \end{pmatrix} \Bigg)^{t/\tau} \vec{a}_0, \end{aligned} \tag{B.18}$$

and

$$\begin{aligned} \vec{b} = \left(Ee^{B\tau}\right)^{t/\tau}\vec{b}_0 = r^{nt/\tau}e^{-\xi t}\Bigg(& \begin{pmatrix} (1-p)e^{-i\phi} & (1-p)e^{i\phi} \\ pe^{-i\phi} & pe^{i\phi} \end{pmatrix}^{\otimes n} \otimes \begin{pmatrix} c_\xi & s_\xi \\ 0 & 0 \end{pmatrix} \\ & + \begin{pmatrix} pe^{-i\phi} & pe^{i\phi} \\ (1-p)e^{-i\phi} & (1-p)e^{i\phi} \end{pmatrix}^{\otimes n} \otimes \begin{pmatrix} 0 & 0 \\ s_\xi & c_\xi \end{pmatrix} \Bigg)^{t/\tau} \vec{b}_0, \end{aligned} \tag{B.19}$$

with

$$re^{\pm i\phi} = e^{-\gamma\tau}(x_\pm + y) = e^{-\gamma\tau}\Big(\cos(\Delta\tau) + \frac{\gamma \pm i\omega}{\Delta}\sin(\Delta\tau)\Big). \tag{B.20}$$

It easy to show using Eq. (B.18) that the final amplitude corresponding to the outer product $|j0\rangle\langle j0|$ is equal to $\frac{(1-p)^{n-h_j}p^{h_j}}{2}$, and similarly the amplitude corresponding to the outer product $|\bar{j}1\rangle\langle\bar{j}1|$ is also equal to $\frac{(1-p)^{n-h_j}p^{h_j}}{2}$ - here h_j is the Hamming weight of the bit string of the sensing qubits, and does not include the

ancillary qubit. The solution to Eq. (B.19) is more complex. After the first round of error correction (and each subsequent round), the amplitude corresponding to the outer product $|j0\rangle\langle\bar{j}1|$ is of the form $\frac{(1-p)^{n-h_j}p^{h_j}Re^{-i\theta}}{2}$, and the amplitude corresponding to the outer product $|\bar{j}1\rangle\langle j0|$ is of the form $\frac{(1-p)^{n-h_j}p^{h_j}Re^{i\theta}}{2}$. By translating the problem to a recurrence relation between $Re^{-i\theta}$ and $Re^{i\theta}$, the problem becomes

$$\begin{aligned}\begin{pmatrix} Re^{-i\theta} \\ Re^{+i\theta} \end{pmatrix} &= r^{nt/\tau}e^{-\xi t}\begin{pmatrix} c_\xi q_- & s_\xi q_+ \\ s_\xi q_- & c_\xi q_+ \end{pmatrix}^N \begin{pmatrix} \upsilon_- \\ \upsilon_+ \end{pmatrix} \\ &= r^{nt/\tau}e^{-\xi t}\left(\frac{\mu_+\mu_-^N - \mu_-\mu_+^N}{\mu_+ - \mu_-}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{\mu_+^N - \mu_-^N}{\mu_+ - \mu_-}\begin{pmatrix} c_\xi q_- & s_\xi q_+ \\ s_\xi q_- & c_\xi q_+ \end{pmatrix}\right)\begin{pmatrix} \upsilon_- \\ \upsilon_+ \end{pmatrix},\end{aligned} \tag{B.21}$$

with $N(nt/\tau - 1)$, and

$$q_\pm = (1-p)e^{\pm i\phi} + pe^{\mp i\phi}, \tag{B.22}$$

$$\mu_\pm = c_\xi \cos\phi \pm \sqrt{q_+q_-s_\xi^2 - (1-2p)^2c_\xi^2\sin^2\phi}, \tag{B.23}$$

$$\upsilon_\pm = c_\xi e^{\pm in\phi} + s_\xi e^{\mp in\phi}. \tag{B.24}$$

In the general setting, with a noisy ancilla and imperfect error correction, the quantum state after time t can be written as

$$\rho = \sum_j \lambda_{j,+}\left|\psi_{j,+}\right\rangle\!\left\langle\psi_{j,+}\right| + \lambda_{j,-}\left|\psi_{j,-}\right\rangle\!\left\langle\psi_{j,-}\right|, \tag{B.25}$$

where

$$\lambda_{j,\pm} = (1-p)^{n-h_j}p^{h_j}\frac{1\pm R}{2}, \tag{B.26}$$

and

$$|\psi_{j,\pm}\rangle = \frac{1}{\sqrt{2}}\big(e^{-i\theta/2}\,|j0\rangle \pm e^{+i\theta/2}\,|\bar{j}1\rangle\big). \tag{B.27}$$

From which, the QFI can be computed

$$\begin{aligned}\mathcal{Q} &= \sum_j\left(\frac{\dot{\lambda}_{j,+}^2}{\lambda_{j,+}} + \frac{\dot{\lambda}_{j,-}^2}{\lambda_{j,-}} + 2\frac{(\lambda_{j,+}-\lambda_{j,-})^2}{\lambda_{j,+}+\lambda_{j,-}}\Big(\left|\,\langle\psi_{j,+}|\dot{\psi}_{j,-}\rangle\,\right|^2 + \left|\,\langle\psi_{j,-}|\dot{\psi}_{j,+}\rangle\,\right|^2\Big)\right) \\ &= \frac{\dot{R}^2}{1-R^2} + R^2\dot{\theta}^2.\end{aligned} \tag{B.28}$$

The various sub-cases are explored in the following subsections.

B.3.1 Ideal Error Correction

The simplest case is when $\xi = 0$ and $p = 0$. In this scenario $Re^{\pm i\theta} = \big(re^{\pm i\phi}\big)^{nt/\tau}$. The QFI simplifies greatly, it can be written in the form

$$\mathcal{Q}_1 = n^2 t^2 r^{2nt/\tau} f, \tag{B.29}$$

where

$$f = \frac{1}{\tau^2}\Big(\frac{1}{1-r^{2nt/\tau}}\frac{\dot{r}^2}{r^2} + \dot{\phi}^2\Big) = 1 - 2\gamma\tau + \frac{7\gamma^2\tau^2}{3} + \frac{4\gamma\tau^2}{3nt} + \mathcal{O}\big(\tau^3\big), \tag{B.30}$$

and

$$r^{2nt/\tau} = 1 - \frac{4}{3}nt\gamma\omega^2\tau^2 + \mathcal{O}\big(\tau^3\big). \tag{B.31}$$

B.3.2 Noisy Ancilla

The second case has a noisy ancillary qubit ($\xi \neq 0$). The analytic expression for $Re^{\pm i\theta}$ is quite complicated; to gauge the effects of the noise a Taylor expansion is performed

$$Re^{\pm i\theta} = (1-\xi t)\big(re^{\pm i\phi}\big)^{nt/\tau} + \xi\tau\frac{\sin(nt\phi/\tau)}{\sin(n\phi)}\big(re^{\mp i\phi}\big)^{n} + \mathcal{O}\big(\xi^2\big). \tag{B.32}$$

Which leads to a QFI of

$$\mathcal{Q}_2 = n^2 t^2 r^{2nt/\tau}(f - g\xi) + \mathcal{O}\big(\xi^2\big), \tag{B.33}$$

where

$$\begin{aligned} g =& \Big(\frac{n\omega t\big(1+3\cos(2n\omega t)\big) + (n^2\omega^2t^2-2)\sin(2n\omega t)}{n^3\omega^3t^3} + 2\Big)t \\ &+ \frac{2\big(n\omega t\cos(n\omega t) - \sin(n\omega t)\big)^2}{n^2\omega^2t^2}\tau \\ &+ \Big(\frac{(4n\omega t - 2n^3\omega^3t^3)\cos(2n\omega t) - (2-5n^2\omega^2t^2)\sin(2n\omega t)}{n^3\omega^3t^3} - 4\Big)\gamma t\tau + \mathcal{O}\big(\tau^2\big). \end{aligned} \tag{B.34}$$

To simplify analysis, the following inequalities are used:

$$\frac{2}{3} \leq \frac{n\omega t\big(1+3\cos(2n\omega t)\big)+(n^2\omega^2t^2-2)\sin(2n\omega t)}{n^3\omega^3t^3}+2 \leq \frac{5}{2}, \tag{B.35}$$

$$0 \leq \frac{2\big(n\omega t\cos(n\omega t)-\sin(n\omega t)\big)^2}{n^2\omega^2t^2} \leq \frac{5}{2}, \tag{B.36}$$

$$-7 \leq \frac{(4n\omega t-2n^3\omega^3t^3)\cos(2n\omega t)-(2-5n^2\omega^2t^2)\sin(2n\omega t)}{n^3\omega^3t^3}-4 \leq 0, \tag{B.37}$$

from which it follows that

$$\Big(\frac{2}{3}-7\gamma\tau\Big)t \leq g+\mathcal{O}\big(\tau^2\big) \leq \frac{5}{2}(t+\tau). \tag{B.38}$$

B.3.3 Imperfect Error Correction

The third case has imperfect syndrome diagnosis ($p \neq 0$). It is straightforward to show

$$Re^{\pm i\theta} = \big(re^{\pm i\phi}\big)^{nt/\tau}\big(q_{\pm}e^{\mp i\phi}\big)^{n(t/\tau-1)}. \tag{B.39}$$

Which leads to a QFI of

$$\mathcal{Q}_3 = n^2t^2(rq)^{2nt/\tau}h, \tag{B.40}$$

with $q^2 = q_+q_-$, which also satisfies

$$q^{2nt/\tau} = 1-4p(1-p)\omega^2t\tau+\mathcal{O}\big(\tau^2\big), \tag{B.41}$$

and

$$h = (1-2p)^2f+4p\Big(\frac{1-p}{n}+1-2p\Big)\frac{\tau}{t}+\mathcal{O}\big(\tau^2\big). \tag{B.42}$$

B.4 QFI Using The Generalized Bit Flip Code

The generalized bit flip code [Got97] does not use an ancillary qubit, instead a global stabilizer measurement is made. The correction made maps the outer product $|j\rangle\langle j|$ to $|0\rangle\langle 0|^{\otimes n}$ if $h_j < n/2$ and $|1\rangle\langle 1|^{\otimes n}$ if $h_j > n/2$ (it is assumed that n is odd to avoid complications when $h_j = n/2$), it similarly maps $|j\rangle\langle\bar{j}|$ to $|0\rangle\langle 1|^{\otimes n}$ if $h_j < n/2$ and $|1\rangle\langle 0|^{\otimes n}$ if $h_j > n/2$. This transformation can (just as with the parity check code) be represented as a matrix E, where $E^{(j,k)}$ is defined to be the entry of E in the jth

row and kth column

$$E^{(j,k)} = \begin{cases} 1, \text{ if } h_j = 0 \text{ and } h_k < \frac{n}{2} \\ 1, \text{ if } h_j = n \text{ and } h_k > \frac{n}{2} \\ 0, \text{ otherwise} \end{cases} . \tag{B.43}$$

Using the same methodology as the parity check code (the main difference being that there is no ancillary qubit), the amplitudes of the final quantum state are given by

$$\vec{a} = \left(Ee^{A\tau}\right)^{t/\tau} \vec{a}_0, \tag{B.44}$$

and,

$$\vec{b} = \left(Ee^{B\tau}\right)^{t/\tau} \vec{b}_0. \tag{B.45}$$

The solution of $\vec{a}$ is trivial; the only non-zero entries are the first and last, both of which are equal to 1/2. The solution for $\vec{b}$ is more complicated, but the only significant terms of the matrix are the four corner entries. By discarding the other entries, a reduced version of the problem is obtained

$$\vec{b'} = \begin{pmatrix} \eta_- & \zeta_+ \\ \zeta_- & \eta_+ \end{pmatrix}^{t/\tau} \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} \tag{B.46}$$

where the first and second entry of $\vec{b'}$ corresponds to the amplitudes of $|0\rangle\langle 1|^{\otimes n}$ and $|1\rangle\langle 0|^{\otimes n}$ respectively, and

$$\eta_\pm = e^{-n\gamma\tau} \sum_{m=0}^{\lfloor n/2 \rfloor} \binom{n}{m} x_\pm^{n-m} y^m, \tag{B.47}$$

$$\zeta_\pm = e^{-n\gamma\tau} \sum_{m=0}^{\lfloor n/2 \rfloor} \binom{n}{m} x_\pm^{m} y^{n-m}, \tag{B.48}$$

and additionally, $\eta_\pm + \zeta_\pm = \left(re^{\pm i\phi}\right)^n$. Because $\zeta_\pm \in \mathcal{O}\left(\tau^{\frac{n+1}{2}}\right)$, it follows that

$$\begin{pmatrix} \eta_- & \zeta_+ \\ \zeta_- & \eta_+ \end{pmatrix}^{t/\tau} = \begin{pmatrix} r^n e^{-ni\phi} & 0 \\ 0 & r^n e^{+ni\phi} \end{pmatrix}^{t/\tau} + \mathcal{O}\left((\tau^{\frac{n-1}{2}}\right). \tag{B.49}$$

Therefore, for large n the final quantum state in this scenario is very similar to the final quantum state using the parity check code (with a noiseless ancilla and perfect

error correction). Mathematically, it is equivalent up to $\mathcal{O}\left(\tau^{\frac{n-1}{2}}\right)$. Thus, the QFI is similarly equivalent up to the same order.

C
Soundness Proofs

C.1 Recurring Mathematical Tools

Before introducing the derivations of the soundness proofs, some frequently recurring tools present in (most of) the proofs are explained here for the sake of organization.

C.1.1 Twirling Lemmas

The first type recurring tool used in the soundness proofs in this Appendix are Clifford twirling lemmas. The Pauli twirling lemma states [Dan+09] that for any m qubit quantum state ρ and Pauli operators $Q, Q' \in \mathcal{P}_m$, with $Q \neq Q'$

$$\sum_{P \in \mathcal{P}_m} PQP\rho PQ'P = 0. \tag{C.1}$$

The reason is that because $Q \neq Q'$, $\mathcal{P}_m$ can be divided into four equal sets. One set of operators which commutes with both Q and Q', one set which commutes Q and anti-commutes with Q', one set which anti-commutes with Q and commutes with Q', and one set which anti-commutes with both Q and Q'. All four of these are equal in size, from which it follows that the above sum is zero.

The proof of the Clifford twirling lemma [Dan+09] is slightly more involved, but the statement is similar: for any m qubit quantum state ρ and Pauli operators $Q, Q' \in \mathcal{P}_m$, with $Q \neq Q'$

$$\sum_{C \in \mathcal{C}_m} CQC^\dagger \rho CQ'C^\dagger = 0. \tag{C.2}$$

The basis of the proof is similar: for any Q and Q' which are not equal and neither of which is the identity, the operators of the Clifford group can be partitioned into sets of four C_a, C_b, C_c, C_d where

$$C_a Q C_a^\dagger = C_b Q C_b^\dagger = -C_c Q C_c^\dagger = -C_d Q C_d^\dagger, \tag{C.3}$$

and

$$C_a Q' C_a^\dagger = -C_b Q' C_b^\dagger = C_c Q' C_c^\dagger = -C_d Q' C_d^\dagger. \tag{C.4}$$

When either one of Q or Q' is the identity, the idea is still true except the corresponding relationship, Eq. (C.3) or Eq. (C.4), is no longer true by definition, $C\mathbb{I}C^\dagger = \mathbb{I}$.

A corollary of the Clifford twirling lemma is that the results still holds when the sum is restricted to locally acting Clifford operators

$$\sum_{C \in \mathcal{C}_1^{\otimes m}} C Q C^\dagger \rho C Q' C^\dagger = 0. \tag{C.5}$$

This is apparent when ρ is written as a sum over the Pauli group P, and all operators are decomposed into locally acting operators

$$\sum_{C \in \mathcal{C}_1^{\otimes m}} C Q C^\dagger \rho C Q' C^\dagger = \frac{1}{2^m} \operatorname{Tr}(P\rho) \sum_{P \in \mathcal{P}_m} \bigotimes_{j=1}^{m} \Big(\sum_{C_j \in \mathcal{C}_1} C_j Q_j C_j^\dagger P C_j Q_j' C_j^\dagger \Big). \tag{C.6}$$

Because $Q \neq Q'$ there exists a j such that $Q_j \neq Q_j'$, the Clifford twirling lemma dictates

$$\sum_{C_j \in \mathcal{C}_1} C_j Q_j C_j^\dagger P_j C_j Q_j' C_j^\dagger = 0, \tag{C.7}$$

and thus the whole sum is zero, proving the locally acting Clifford twirling lemma. Note that P_j not being a quantum state is irrelevant to the proof of the Clifford twirl.

C.1.2 CPTP Representation Of A Malicious Attack

Another recurring mathematical tool used in the soundness proofs is to represent an arbitrary attack as a CPTP map Γ, which can be expanded in terms of a Kraus decomposition $\{A_\alpha\}$

$$\rho \to \Gamma(\rho) = \sum_\alpha A_\alpha \rho A_\alpha^\dagger, \tag{C.8}$$

where $\sum_\alpha A_\alpha A_\alpha^\dagger = \mathbb{I}$. Next, a m dimensional Kraus operator can be written with respect to the Pauli basis

$$A_\alpha = \sum_{P \in \mathcal{P}_m} a_{\alpha,P} P, \tag{C.9}$$

where $a_{\alpha,P} = 2^{-m} \operatorname{Tr}(P A_\alpha)$. Therefore, in the Pauli representation, the action of Γ is

$$\Gamma(\rho) = \sum_\alpha \sum_{P,Q} a_{\alpha,P} a^*_{\alpha,Q} P \rho Q, \tag{C.10}$$

where the asterisk denotes the complex conjugate. The completeness relationship reads

$$\sum_\alpha \sum_{P \in \mathcal{P}_m} |a_{\alpha,P}|^2 = 1. \tag{C.11}$$

C.2 Unsecured Quantum Channel

For this protocol, we assume that the ideal output state ρ_{id}[1] is a pure state. This is logical assumption since pure states are superior candidates as a resource for quantum metrology. In doing so, the fidelity component of the soundness is equal to trace, greatly simplifying the expression

$$\begin{aligned} &\frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} p_{\text{acc}}(k,\Gamma) \cdot \Big(1 - \mathscr{F}\big(\rho_{\text{id}}, \rho_{\text{out}}(k,\Gamma)\big)\Big) \\ =&\frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} p_{\text{acc}}(k,\Gamma) \cdot \Big(1 - \operatorname{Tr}\big(\rho_{\text{id}} \rho_{\text{out}}(k,\Gamma)\big)\Big) \\ =&\frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} \operatorname{Tr}\Big(\Pi_{\text{acc}}(k) \rho_f(k,\Gamma)\Big), \end{aligned} \tag{C.12}$$

where $\rho_f(k,\Gamma)$ is understood as the final ensemble of both ancillary flag qubits and the qubits intended for quantum metrology, and $\Pi_{\text{acc}}(k)$ projects the ancillary flag qubits onto the 'accept state', and the qubits intended for quantum metrology onto $\mathbb{I} - \rho_{\text{id}}$.

[1] We make this assumption for both the single use of the quantum channel, and the double use of the quantum channel.

C.2.1 Trap Code (Single Use)

When using the trap code, there are a total of $\left|\mathcal{K}\right| = \left|\mathcal{C}_1^{\otimes m}\right|\binom{m}{t}$ possible classical keys; describing both the choices k and ℓ. The projector $\Pi_{\text{acc}}(k)$ depends only on the choice of ℓ and is independent of the choice of encryption operation C. But for all intents and purposes, it can be expressed as $\Pi_{\text{acc}}(\ell) = \pi(\ell)\Pi\pi(\ell)^\dagger$ where $\pi(\ell)$ is the permutation corresponding to the random placement of the flag qubits and

$$\Pi = (\mathbb{I} - \rho) \otimes |0\rangle\langle 0|^{\otimes t}. \tag{C.13}$$

Upon receipt and decryption by Bob, the quantum state for a specific key k and attack Γ is

$$\rho_f(k, \Gamma) = C^\dagger \Gamma\big(C\rho_{\text{in},\ell}C^\dagger\big)C, \tag{C.14}$$

where $\rho_{\text{in},\ell} = \pi(\ell)\rho \otimes |0\rangle\langle 0|^{\otimes t}\,\pi(\ell)^\dagger$. Thus the soundness is a bound on the quantity

$$\frac{1}{\binom{m}{t}|\mathcal{C}_1|^m}\sum_{\ell}\sum_{C\in\mathcal{C}_1^{\otimes m}} \text{Tr}\left(\Pi\pi(\ell)^\dagger\rho_f(k,\Gamma)\pi(\ell)\right). \tag{C.15}$$

Because of the linearity of the trace, the sum over C can be brought into the trace, which is simplified by expanding Γ into a Kraus decomposition and the locally acting Clifford twirling lemma

$$\begin{aligned}
\sum_{C\in\mathcal{C}_1^{\otimes m}} \rho_f(k,\Gamma) &= \sum_{C\in\mathcal{C}_1^{\otimes m}}\sum_{\alpha} C^\dagger A_\alpha C\rho_{\text{in},\ell}C^\dagger A_\alpha^\dagger C \\
&= \sum_{C\in\mathcal{C}_1^{\otimes m}}\sum_{\alpha}\sum_{P_1,P_2\in\mathcal{P}_m} a_{\alpha,P_1}a^*_{\alpha,P_2}C^\dagger P_1 C\rho_{\text{in},\ell}C^\dagger P_2 C \\
&= \sum_{C\in\mathcal{C}_1^{\otimes m}}\sum_{\alpha}\sum_{P\in\mathcal{P}_m} |a_{\alpha,P}|^2 C^\dagger PC\rho_{\text{in},\ell}C^\dagger PC.
\end{aligned} \tag{C.16}$$

The next simplification uses the fact that the single qubit Clifford group $\mathcal{C}_1$ maps any non-identity Pauli into an equal distribution over the set $\{\pm X, \pm Y, \pm Z\}$. It then follows that if P has $d(P)$ non-identity terms, then $CPC^\dagger$ is a similar Pauli operator $\tilde{P}$ (with a phase of ± 1). Specifically, $\tilde{P}$ has the same number of non-identity terms which are indexed by the same positions as the non-identity terms of P. The notion of 'similarity' is denoted using $\sim$, for example $\mathbb{I}\otimes X \sim \mathbb{I}\otimes Y \sim \mathbb{I}\otimes Z$. Thus,

$$\frac{1}{|\mathcal{C}_1|^m}\sum_{C\in\mathcal{C}_1^{\otimes m}}\rho_f(k,\Gamma) = \sum_{\alpha}\sum_{P\in\mathcal{P}_m}\frac{|a_{\alpha,P}|^2}{3^{d(P)}}\sum_{\tilde{P}\sim P}\tilde{P}\rho_{\text{in},\ell}\tilde{P}. \tag{C.17}$$

Combining everything thus far

$$\begin{aligned}&\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}\mathrm{Tr}\left(\Pi_{\mathrm{acc}}(k)\rho_f(k,\Gamma)\right)\\=&\frac{1}{\binom{m}{t}}\sum_{\ell}\sum_{\alpha}\sum_{P\in\mathcal{P}_m}\frac{|a_{\alpha,P}|^2}{3^{d(P)}}\sum_{\tilde{P}\sim P}\mathrm{Tr}\left(\Pi\pi(\ell)^\dagger\tilde{P}\pi(\ell)\rho\otimes|0\rangle\langle 0|^{\otimes t}\,\pi(\ell)^\dagger\tilde{P}\pi(\ell)\right).\end{aligned}\tag{C.18}$$

If $d(P)=0$, then P is identically the identity and the trace is zero. For any $d(P)>0$ and $s\leq d(P)$, there are $\binom{m-d(P)}{t-s}$ permutations ℓ where the non-identity terms of P interact with s trap qubits. The only $\tilde{P}$ which results in a non-zero trace is the unique possibility of Z acting on all the s trap qubits. Additionally, when $d(P)\leq t$ and $s=d(P)$ the trace is identically zero, since the Pauli is uniquely acting on the qubits intended for quantum metrology. Otherwise, the trace onto the first n qubits can be bounded by 1. Hence,

$$\begin{aligned}\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}\mathrm{Tr}\left(\Pi_{\mathrm{acc}}(k)\rho_f(k,\Gamma)\right)&\leq\sum_{\alpha}\sum_{P\in\mathcal{P}_m}|a_{\alpha,P}|^2\sum_{s=0}^{s_{\max}}\frac{1}{3^s}\frac{\binom{m-d(P)}{t-s}}{\binom{m}{t}}\\&=\frac{1}{\binom{m}{t}}\sum_{r=1}^{m}c_r\sum_{s=0}^{s_{\max}}\frac{1}{3^s}\frac{\binom{m-r}{t-s}}{\binom{m}{t}}.\end{aligned}\tag{C.19}$$

where $d(P)$ has been replaced by r as it is no longer dependent on a specific Pauli P, $s_{\max}=r-1$ if $r\leq t$ and $s_{\max}=t$ otherwise, and c_r is the sum of all $|a_{\alpha,P}|^2$ with r total non-identity indices spanned by P. The completeness relationship, Eq. (C.11), guarantees that $c_r\leq 1$. Using the upper bound for c_r and swapping the sums of s

and r, the inequality becomes

$$\begin{aligned}
\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}\mathrm{Tr}\left(\Pi_{\mathrm{acc}}(k)\rho_f(k,\Gamma)\right) &\leq \frac{1}{\binom{m}{t}}\sum_{s=0}^{t}\left(\frac{1}{3}\right)^s\sum_{r=s+1}^{m}\binom{m-r}{t-s}\\
&= \frac{1}{\binom{m}{t}}\sum_{s=0}^{t}\left(\frac{1}{3}\right)^s\binom{m-s}{t-s+1}\\
&= \frac{m-t}{t+1}\sum_{s=0}^{t}\left(\frac{1}{3}\right)^s\frac{(t+1)!(m-s)!}{(t-s+1)!m!}\\
&= \frac{m-t}{t+1}+\frac{m-t}{t+1}\sum_{s=1}^{t}\left(\frac{1}{3}\right)^s\prod_{j=0}^{s-1}\frac{t+1-j}{m-j}\\
&\leq \frac{m-t}{t+1}+\frac{m-t}{t+1}\sum_{s=1}^{t}\left(\frac{1}{3}\right)^s\left(\frac{t+1}{m}\right)^s\\
&\leq \frac{3}{2}\frac{m-t}{t}.
\end{aligned} \tag{C.20}$$

C.2.2 Clifford Code (Single Use)

Using the Clifford code, the key is solely dependent on the choice of $C \in \mathcal{C}_m$. The projector $\Pi_{\mathrm{acc}}(k) = (\mathbb{I}-\rho)\otimes|0\rangle\langle 0|^{\otimes t}$ is independent from this choice.

The derivation begins in a similar fashion to that of the trap code, where the output quantum state is simplified using the Clifford twirling lemma

$$\sum_{C\in\mathcal{C}_1^{\otimes m}}\rho_f(C,\Gamma) = \sum_{C\in\mathcal{C}_m}\sum_{\alpha}\sum_{P\in\mathcal{P}_m}|a_{\alpha,P}|^2 C^\dagger PC\rho_{\mathrm{in}}C^\dagger PC. \tag{C.21}$$

However, in this case the above can be further simplified as the Clifford group maps any non-identity Pauli uniformly to all other non-identity Pauli operators (up to a phase of ± 1)

$$\frac{1}{|\mathcal{C}_m|}\sum_{C\in\mathcal{C}_m}C^\dagger PC\rho C^\dagger PC = \frac{1}{|\mathcal{P}_m|-1}\sum_{P'\neq\mathbb{I}\in\mathcal{P}_m}P'\rho P' = \frac{1}{4^m-1}(2^m\mathbb{I}-\rho). \tag{C.22}$$

Denoting $a = \sum_\alpha |a_{\alpha,\mathbb{I}}|^2$, the expected final state is

$$\frac{1}{|\mathcal{C}_m|}\sum_{C\in\mathcal{C}_m}\rho_f(C,\Gamma) = a\rho_{\mathrm{in}} + \frac{1-a}{4^m-1}(2^m\mathbb{I}-\rho_{\mathrm{in}}), \tag{C.23}$$

from which it follows that

$$\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}\mathrm{Tr}\left(\Pi_{\mathrm{acc}}(k)\rho_f(k,\Gamma)\right)=\left(a-\frac{1-a}{4^m-1}\right)\mathrm{Tr}\left(\Pi\rho_{\mathrm{in}}\right)+2^m\frac{1-a}{4^m-1}\mathrm{Tr}\left(\Pi\right). \quad \text{(C.24)}$$

The first trace is null because $\mathrm{Tr}\left((\mathbb{I}-\rho)\rho\right)=0$ and the second trace is equal to $2^{m-t}-1$, hence

$$\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}\mathrm{Tr}\left(\Pi_{\mathrm{acc}}(k)\rho_f(k,\Gamma)\right)\leq\frac{2^m(2^{m-t}-1)}{4^m-1}\leq\frac{2^m\cdot 2^{m-t}}{4^m}\leq 2^{-t}. \quad \text{(C.25)}$$

C.2.3 Trap Code (Double Use)

In the double use of the quantum channel, depicted in Fig. (6.3), a malicious eavesdropper can interact with the quantum channel twice. These interactions can both be represented as CPTP maps, Γ_1 and Γ_2. For the trap code, the set of keys is now comprised of the random placement of the flags ℓ, and two Clifford operations $C_1, C_2 \in \mathcal{C}_1^{\otimes m}$. The projector $\Pi_{\mathrm{acc}}(k)$ is once again of the form $\pi(\ell)\Pi\pi(\ell)^\dagger$, with the change that Π projects onto the encoded quantum state (which is still assumed to be a pure state)

$$\Pi=(\mathbb{I}-\Lambda_\theta(\rho))\otimes|0\rangle\langle 0|^{\otimes t} \quad \text{(C.26)}$$

After undergoing the final decryption by Alice, the final quantum state for a specific key k and attacks Γ_1 and Γ_2 is given by

$$\rho_f(k,\Gamma)=C_2^\dagger\Gamma_2\big(C_2\Lambda_\theta^{(\ell)}\big(C_1^\dagger\Gamma_2\big(C_1\rho_{\mathrm{in},\ell}C_1^\dagger\big)C_1\big)C_2^\dagger\big)C_2, \quad \text{(C.27)}$$

where $\Lambda_\theta^{(\ell)}$ is the parameter encoding operation which only acts on the qubits intended for quantum metrology, if σ is an m dimensional quantum state then

$$\Lambda_\theta^{(\ell)}(\sigma)=\pi(\ell)\big(\Lambda_\theta\otimes\mathbb{I}\big)\big(\pi(\ell)^\dagger\sigma\pi(\ell)\big)\pi(\ell)^\dagger, \quad \text{(C.28)}$$

where the identity term in the above equation represents the identity channel acting on the final t qubits. Using the same techniques used in the trap code (single use) proof, the sum over C_1 and C_2 can be brought into the trace. By representing Γ_1 and Γ_2 using Kraus decomposition $\{A_\alpha\}$ and $\{B_\beta\}$ respectively, and further reducing these operators in the Pauli basis, the sum over C_1 and C_2 is greatly simplified thanks

to the local Clifford twirling lemmas

$$\begin{aligned}&\sum_{C_1,C_2\in\mathcal{C}_1^{\otimes m}}\rho_f(k,\Gamma)\\ =&\sum_{C_1,C_2\in\mathcal{C}_1^{\otimes m}}\sum_{\alpha,\beta}\sum_{P,Q\in\mathcal{P}_m}|a_{\alpha,P}|^2|b_{\beta,Q}|^2C_2^\dagger QC_2\Lambda_\theta^{(\ell)}\big(C_1^\dagger PC_1\rho_{\text{in},\ell}C_1^\dagger PC_1\big)C_2^\dagger QC_2,\end{aligned}\tag{C.29}$$

where $a_{\alpha,P}=\text{Tr}(A_\alpha P)$ and $b_{\beta,Q}=\text{Tr}(B_\beta Q)$, which satisfy the completeness relationships $\sum_{\alpha,P}|a_{\alpha,P}|^2=\sum_{\beta,Q}|b_{\beta,Q}|^2=1$. This is once again simplified using the notation of similar Pauli operators

$$\frac{1}{|\mathcal{C}_1|^{2m}}\sum_{C_1,C_2\in\mathcal{C}_1^{\otimes m}}\rho_f(\Gamma)=\sum_{\alpha,\beta}\sum_{P,Q\in\mathcal{P}_m}\frac{|a_{\alpha,P}|^2|b_{\beta,Q}|^2}{3^{d(P)+d(Q)}}\sum_{\substack{\tilde{P}\sim P\\ \tilde{Q}\sim Q}}\tilde{Q}\Lambda_\theta^{(\ell)}\big(\tilde{P}\rho_{\text{in},\ell}\tilde{P}\big)\tilde{Q}.\tag{C.30}$$

Combining everything thus far

$$\begin{aligned}&\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}\text{Tr}\Big(\Pi_{\text{acc}}(k)\rho_f(k,\Gamma)\Big)\\ =&\frac{1}{\binom{m}{t}}\sum_{\ell}\sum_{\alpha,\beta}\sum_{P,Q\in\mathcal{P}_m}\frac{|a_{\alpha,P}|^2|b_{\beta,Q}|^2}{3^{d(P)+d(Q)}}\sum_{\substack{\tilde{P}\sim P\\ \tilde{Q}\sim Q}}\text{Tr}\Big(\Pi\pi(\ell)\tilde{Q}\Lambda_\theta^{(\ell)}\big(\tilde{P}\rho_{\text{in},\ell}\tilde{P}\big)\tilde{Q}\pi(\ell)^\dagger\Big).\end{aligned}\tag{C.31}$$

To simplify the above expression, we use a slightly different argument to the protocol for the single use case. This time we define r to be the number of non-identity indices spanned by P or Q. For example the total number of non-identity indices spanned by $P=\mathbb{I}\otimes X\otimes Z$ and $Q=\mathbb{I}\otimes X\otimes\mathbb{I}$ is $r=2$. Again, for any $s\leq r$, there are $\binom{m-r}{t-s}$ permutations of the trap qubits where the non-identity indices spanned by P or Q interact with s trap qubits. The number of $\tilde{P}$ and $\tilde{Q}$ which results in an accepted outcome is less than $(\frac{5}{9})^s\cdot 3^{d(P)+d(Q)}$. This is because when the non-identity terms of $\tilde{P}$ and $\tilde{Q}$ do not overlap, the only accepted Pauli is Z (which is $1/3<5/9$ of the possibilities), however, when there is overlap at said index, the Pauli's which are accepted are ZZ, XX, YY, XY and YX (which is $5/9$ of the possibilities). The orthogonal compliment portion of the projector Π is again equal to zero when all of the r non-identity terms interact with the trap qubits. Mathematically, in this

version of the protocol, we obtain

$$\begin{aligned}\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}\mathrm{Tr}\left(\Pi_{\mathrm{acc}}(k)\rho_f(k,\Gamma)\right) &\leq \sum_{\alpha,\beta}\sum_{P,Q}|a_{\alpha,P}|^2|b_{\beta,Q}|^2\sum_{s=0}^{s_{\max}}\left(\frac{5}{9}\right)^s\frac{\binom{m-r}{t-s}}{\binom{m}{t}}\\ &= \sum_{r=0}^{m}c_r\sum_{s=0}^{s_{\max}}\left(\frac{5}{9}\right)^s\frac{\binom{m-r}{t-s}}{\binom{m}{t}},\end{aligned} \tag{C.32}$$

once again $s_{\max} = r-1$ for $r \leq t$ and $s_{\max} = t$ otherwise, and here $c_r \leq 1$ is the sum of all $|a_{\alpha,P}|^2|b_{\beta,Q}|^2$ with r total non-identity indices spanned by P and Q. Using the upper bound for c_r and swapping the sums of s and r we obtain

$$\begin{aligned}\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}\mathrm{Tr}\left(\Pi_{\mathrm{acc}}(k)\rho_f(k,\Gamma)\right) &\leq \frac{1}{\binom{m}{t}}\sum_{s=0}^{t}\left(\frac{5}{9}\right)^s\sum_{r=s+1}^{m}\binom{m-r}{t-s}\\ &= \frac{1}{\binom{m}{t}}\sum_{s=0}^{t}\left(\frac{5}{9}\right)^s\binom{m-s}{t-s+1}\\ &= \frac{m-t}{t+1}\sum_{s=0}^{t}\left(\frac{5}{9}\right)^s\frac{(t+1)!(m-s)!}{(t-s+1)!m!}\\ &= \frac{m-t}{t+1}+\frac{m-t}{t+1}\sum_{s=1}^{t}\left(\frac{5}{9}\right)^s\prod_{j=0}^{s-1}\frac{t+1-j}{m-j}\\ &\leq \frac{m-t}{t+1}+\frac{m-t}{t+1}\sum_{s=1}^{t}\left(\frac{5}{9}\right)^s\left(\frac{t+1}{m}\right)^s\\ &\leq \frac{9}{4}\frac{m-t}{t+1}\\ &\leq \frac{9}{4}\frac{m-t}{t}.\end{aligned} \tag{C.33}$$

C.2.4 Clifford Code (Double Use)

In the double use of the quantum channel, the soundness derivation for the Clifford code is very similar to the proof in the single use case. Simplification using the Clifford twirling lemma leads to the expression

$$\begin{aligned}&\sum_{C_1,C_2\in\mathcal{C}_m}\rho_f(k,\Gamma)\\ &= \sum_{C_1,C_2\in\mathcal{C}_m}\sum_{\alpha,\beta}\sum_{P,Q\in\mathcal{P}_m}|a_{\alpha,P}|^2|b_{\beta,Q}|^2C_2^\dagger QC_2\Lambda_\theta\big(C_1^\dagger PC_1\rho_{\mathrm{in}}C_1^\dagger PC_1\big)C_2^\dagger QC_2,\end{aligned} \tag{C.34}$$

where it is understood that Λ_θ acts exclusively on the first n qubits. Define $a = \sum_\alpha |a_{\alpha,\mathbb{I}}|^2$ and $b = \sum_\beta |a_{\beta,\mathbb{I}}|^2$. Using the same logic introduced in the single use case, the expected final state is

$$\begin{aligned}&\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}\rho_f(k,\Gamma)\\ =&\Big(ab - \frac{a(1-b)+b(1-a)}{4^m-1} + \frac{(1-a)(1-b)}{(4^m-1)^2}\Big)\Lambda_\theta\big(\rho_{\text{in}}\big)\\ &+\frac{(1-a)b+a(1-b)}{4^m-1}2^m\mathbb{I}.\end{aligned} \tag{C.35}$$

Because

$$\max_{0\le a,b\le 1}\big((1-a)b+a(1-b)\big) = 1, \tag{C.36}$$

it follows that

$$\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}\text{Tr}\left(\Pi_{\text{acc}}(k)\rho_f(k,\Gamma)\right) = \frac{(1-a)b+a(1-b)}{4^m-1}2^m(2^{m-t}-1) \le \frac{1}{2^t}. \tag{C.37}$$

C.3 Delegated Measurements

After post-processing, the measurement result Alice receives stems from the measurement statistics of

$$\pi^\dagger C^\dagger \mathcal{M}\big(\tilde{\rho} = \Gamma(C\pi\rho_{\text{in}}\pi^\dagger C^\dagger)\big)C\pi, \tag{C.38}$$

where $\mathcal{M}$ corresponds to measuring the quantum states in the basis of $C(P^{\otimes n}\otimes Z^{\otimes t})C^\dagger$. If $\mathcal{M}_{\text{id}}$ is the measurement with respect to the basis of $P^{\otimes n}\otimes Z^{\otimes t}$, then

$$\mathcal{M}(\sigma) = C\pi\mathcal{M}_{\text{id}}(\pi^\dagger C^\dagger\sigma C\pi)\pi^\dagger C^\dagger, \tag{C.39}$$

and thus, after post-processing, the measurement result Alice receives stems from the measurement statistics of

$$\mathcal{M}_{\text{id}}\big(\pi^\dagger C^\dagger\Gamma(C\pi\rho_{\text{in}}\pi^\dagger C^\dagger)C\pi\big). \tag{C.40}$$

Suppose that Alice accepts measurement results, then the remaining measurement statistics will be of the form $\bar{\mathcal{M}}_{\text{id}}(\rho_{\text{out}}(k,\Gamma)$, where $\bar{\mathcal{M}}_{\text{id}}$ is restricted to the measurement results of the n qubits for quantum metrology. The fidelity term in

the soundness is bounded

$$\mathscr{F}\Big(\bar{\mathcal{M}}_{\mathrm{id}}\big(\rho_{\mathrm{id}}\big),\bar{\mathcal{M}}_{\mathrm{id}}\big(\rho_{\mathrm{out}}(k,\Gamma)\big)\Big)\geq\mathscr{F}\Big(\rho_{\mathrm{id}},\rho_{\mathrm{out}}(k,\Gamma)\Big)=\mathrm{Tr}\left(\rho_{\mathrm{id}}\rho_{\mathrm{out}}(k,\Gamma)\right),\quad\text{(C.41)}$$

due to the monotonicity of the fidelity. Thus, the soundness is again bounded by the quantity

$$\begin{aligned}&\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}p_{\mathrm{acc}}(k,\Gamma)\cdot\Big(1-\mathscr{F}\big(\mathcal{M}_1(\rho_{\mathrm{id}}),\mathcal{M}_1(\rho_{\mathrm{out}}(k,\Gamma))\big)\Big)\\ \leq&\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}p_{\mathrm{acc}}(k,\Gamma)\cdot\Big(1-\mathrm{Tr}\left(\rho_{\mathrm{id}}\rho_{\mathrm{out}}(k,\Gamma)\right)\Big)\\ =&\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}\mathrm{Tr}\left(\Pi_{\mathrm{acc}}(k)\rho_f(k,\Gamma)\right).\end{aligned}\quad\text{(C.42)}$$

The same notation is used here as in Eq. (C.12), where

$$\rho_f(k,\Gamma)=\pi^\dagger C^\dagger\Gamma(C\pi\rho_{\mathrm{in}}\pi^\dagger C^\dagger)C\pi\quad\text{(C.43)}$$

is understood as the ensemble of both ancillary flag qubits and the qubits intended for quantum metrology from which the measurement statistics are derived from, and

$$\Pi_{\mathrm{acc}}(k)=\Pi=(\mathbb{I}-\rho_{\mathrm{id}})\otimes|0\rangle\langle 0|^{\otimes t}\quad\text{(C.44)}$$

projects the ancillary flag qubits onto the 'accept state', and the qubits intended for quantum metrology onto $\mathbb{I}-\rho_{\mathrm{id}}$. More specifically, this combination of $\rho_f(k,\Gamma)$ and $\Pi_{\mathrm{acc}}(k)$ is equivalent to that of the soundness derivaiton for the single use of the trap code over a quantum channel, and thus the same techniques mathematical techniques can be applied to find that the soundness is bounded by $\frac{3n}{2t}$.

Bibliography

[Aar09] S. Aaronson, "Quantum copy-protection and quantum money," in *2009 24th Annual IEEE Conference on Computational Complexity*, IEEE, 2009, pp. 229–242.

[Aas+13] J. Aasi, J. Abadie, B. Abbott, R. Abbott, T. Abbott, M. Abernathy, C. Adams, T. Adams, P. Addesso, R. Adhikari, *et al.*, "Enhanced sensitivity of the ligo gravitational wave detector by using squeezed states of light," *Nature Photonics*, vol. 7, no. 8, pp. 613–619, 2013.

[Abb+16] B. P. Abbott, R. Abbott, T. Abbott, M. Abernathy, F. Acernese, K. Ackley, C. Adams, T. Adams, P. Addesso, R. Adhikari, *et al.*, "Observation of gravitational waves from a binary black hole merger," *Physical Review Letters*, vol. 116, no. 6, p. 061 102, 2016.

[Abi+21] B. Abi, T. Albahri, S. Al-Kilani, D. Allspach, L. Alonzi, A. Anastasi, A. Anisenkov, F. Azfar, K. Badgley, S. Baeßler, *et al.*, "Measurement of the positive muon anomalous magnetic moment to 0.46 ppm," *Physical Review Letters*, vol. 126, no. 14, p. 141 801, 2021.

[Ací+18] A. Acín, I. Bloch, H. Buhrman, T. Calarco, C. Eichler, J. Eisert, D. Esteve, N. Gisin, S. J. Glaser, F. Jelezko, *et al.*, "The quantum technologies roadmap: A european community view," *New Journal of Physics*, vol. 20, no. 8, p. 080 201, 2018.

[AFD19] F. Albarelli, J. F. Friel, and A. Datta, "Evaluating the holevo cramér-rao bound for multiparameter quantum metrology," *Physical Review Letters*, vol. 123, no. 20, p. 200 503, 2019.

[AG04] S. Aaronson and D. Gottesman, "Improved simulation of stabilizer circuits," *Physical Review A*, vol. 70, no. 5, p. 052 328, 2004.

[Aha+17] D. Aharonov, M. Ben-Or, E. Eban, and U. Mahadev, "Interactive proofs for quantum computations," *arXiv preprint arXiv:1704.04487*, 2017.

[AK17] K. Azuma and G. Kato, "Aggregating quantum repeaters for the quantum internet," *Physical Review A*, vol. 96, no. 3, p. 032 332, 2017.

[Alb+18] F. Albarelli, M. A. Rossi, D. Tamascelli, and M. G. Genoni, "Restoring heisenberg scaling in noisy quantum metrology by monitoring the environment," *Quantum*, vol. 2, p. 110, 2018.

[Ama16] S.-i. Amari, *Information geometry and its applications*. Springer, 2016, vol. 194.

[Amb+04] A. Ambainis, H. Buhrman, Y. Dodis, and H. Rohrig, "Multiparty quantum coin flipping," in *Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004.*, IEEE, 2004, pp. 250–259.

[Aok+09] T. Aoki, G. Takahashi, T. Kajiya, J.-i. Yoshikawa, S. L. Braunstein, P. Van Loock, and A. Furusawa, "Quantum error correction beyond qubits," *Nature Physics*, vol. 5, no. 8, pp. 541–546, 2009.

[App+09] J. Appel, P. J. Windpassinger, D. Oblak, U. B. Hoff, N. Kjærgaard, and E. S. Polzik, "Mesoscopic atomic entanglement for precision measurements beyond the standard quantum limit," *Proceedings of the National Academy of Sciences*, vol. 106, no. 27, pp. 10 960–10 965, 2009.

[AR15] S. Alipour and A. Rezakhani, "Extended convexity of quantum fisher information in quantum metrology," *Physical Review A*, vol. 91, no. 4, p. 042 104, 2015.

[Arr+14] G. Arrad, Y. Vinkler, D. Aharonov, and A. Retzker, "Increasing sensing resolution with error correction," *Physical Review Letters*, vol. 112, no. 15, p. 150 801, 2014.

[Aru+19] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.

[Aug+16] R. Augusiak, J. Kołodyński, A. Streltsov, M. N. Bera, A. Acin, and M. Lewenstein, "Asymptotic role of entanglement in quantum metrology," *Physical Review A*, vol. 94, no. 1, p. 012 339, 2016.

[Bal04] M. A. Ballester, "Estimation of unitary quantum operations," *Physical Review A*, vol. 69, no. 2, p. 022 303, 2004.

[Bar+02] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp, "Authentication of quantum messages," in *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.*, IEEE, 2002, pp. 449–458.

[Bar+11] J. T. Barreiro, M. Müller, P. Schindler, D. Nigg, T. Monz, M. Chwalla, M. Hennrich, C. F. Roos, P. Zoller, and R. Blatt, "An open-system quantum simulator with trapped ions," *Nature*, vol. 470, no. 7335, pp. 486–491, 2011.

[Bar+12] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, "Demonstration of blind quantum computing," *science*, vol. 335, no. 6066, pp. 303–308, 2012.

[Bar+15] S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J. H. Shapiro, and S. Pirandola, "Microwave quantum illumination," *Physical Review Letters*, vol. 114, no. 8, p. 080 503, 2015.

[BB84] C. H. Bennett and G. Brassard, *Proceedings of the ieee international conference on computers, systems and signal processing*, 1984.

[BC94] S. L. Braunstein and C. M. Caves, "Statistical distance and the geometry of quantum states," *Physical Review Letters*, vol. 72, no. 22, p. 3439, 1994.

[BCK15] J. B. Brask, R. Chaves, and J. Kołodyński, "Improved quantum magnetometry beyond the standard quantum limit," *Physical Review X*, vol. 5, no. 3, p. 031 010, 2015.

[BCR86] O. E. Barndorff-Nielsen, D. R. Cox, and N. Reid, "The role of differential geometry in statistical theory," *International Statistical Review/Revue Internationale de Statistique*, pp. 83–96, 1986.

[BD16] T. Baumgratz and A. Datta, "Quantum enhanced estimation of a multidimensional field," *Physical Review Letters*, vol. 116, no. 3, p. 030 801, 2016.

[Ben+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Physical Review Letters*, vol. 70, no. 13, p. 1895, 1993.

[Ben+96] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Physical Review A*, vol. 54, no. 5, p. 3824, 1996.

[Ben80] P. Benioff, "The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines," *Journal of Statistical Physics*, vol. 22, no. 5, pp. 563–591, 1980.

[Ber+09] D. W. Berry, B. L. Higgins, S. D. Bartlett, M. W. Mitchell, G. J. Pryde, and H. M. Wiseman, "How to perform the most accurate possible phase measurements," *Physical Review A*, vol. 80, no. 5, p. 052 114, 2009.

[Ber+15] D. W. Berry, M. Tsang, M. J. Hall, and H. M. Wiseman, "Quantum bell-ziv-zakai bounds and heisenberg limits for waveform estimation," *Physical Review X*, vol. 5, no. 3, p. 031 018, 2015.

[Ber13] K. Berrada, "Non-markovian effect on the precision of parameter estimation," *Physical Review A*, vol. 88, no. 3, p. 035 806, 2013.

[BFK09] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation," in *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, IEEE, 2009, pp. 517–526.

[BG00] O. E. Barndorff-Nielsen and R. D. Gill, "Fisher information in quantum statistics," *Journal of Physics A: Mathematical and General*, vol. 33, no. 24, p. 4481, 2000.

[BGS13] A. Broadbent, G. Gutoski, and D. Stebila, "Quantum one-time programs," in *Annual Cryptology Conference*, Springer, 2013, pp. 344–360.

[Bha+21] K. Bharti, A. Cervera-Lierta, T. H. Kyaw, T. Haug, S. Alperin-Lea, A. Anand, M. Degroote, H. Heimonen, J. S. Kottmann, T. Menke, *et al.*, "Noisy intermediate-scale quantum (nisq) algorithms," *arXiv preprint arXiv:2101.08448*, 2021.

[Bit96] M. Bitbol, *Schrödinger's philosophy of quantum mechanics*. Springer Science & Business Media, 1996, vol. 188.

[BM06] H. Bombín and M. A. Martin-Delgado, "Topological quantum distillation," *Physical Review Letters*, vol. 97, no. 18, p. 180 501, 2006.

[BM07] H. Bombín and M. A. Martin-Delgado, "Optimal resources for topological two-dimensional stabilizer codes: Comparative study," *Physical Review A*, vol. 76, no. 1, p. 012 305, 2007.

[BMZ87] B.-Z. Bobrovsky, E. Mayer-Wolf, and M. Zakai, "Some classes of global cramér-rao bounds," *The Annals of Statistics*, pp. 1421–1438, 1987.

[Boi+07] S. Boixo, S. T. Flammia, C. M. Caves, and J. M. Geremia, "Generalized limits for single-parameter quantum estimation," *Physical Review Letters*, vol. 98, no. 9, p. 090 401, 2007.

[Boz+18] M. Bozzio, A. Orieux, L. T. Vidarte, I. Zaquine, I. Kerenidis, and E. Diamanti, "Experimental investigation of practical unforgeable quantum money," *npj Quantum Information*, vol. 4, no. 1, pp. 1–8, 2018.

[BP+02] H.-P. Breuer, F. Petruccione, *et al.*, *The theory of open quantum systems*. Oxford University Press on Demand, 2002.

[BPP08] A. Bendersky, F. Pastawski, and J. P. Paz, "Selective and efficient estimation of parameters for quantum process tomography," *Physical Review Letters*, vol. 100, no. 19, p. 190 403, 2008.

[Bra+18] D. Braun, G. Adesso, F. Benatti, R. Floreanini, U. Marzolino, M. W. Mitchell, and S. Pirandola, "Quantum-enhanced measurements without entanglement," *Reviews of Modern Physics*, vol. 90, no. 3, p. 035 006, 2018.

[BS13] J. Borregaard and A. S. Sørensen, "Near-heisenberg-limited atomic clocks in the presence of decoherence," *Physical Review Letters*, vol. 111, no. 9, p. 090 801, 2013.

[BS16] A. Broadbent and C. Schaffner, "Quantum cryptography beyond quantum key distribution," *Designs, Codes and Cryptography*, vol. 78, no. 1, pp. 351–382, 2016.

[BS84] R. S. Bondurant and J. H. Shapiro, "Squeezed states in phase-sensing interferometers," *Physical Review D*, vol. 30, no. 12, p. 2548, 1984.

[Bur69] D. Bures, "An extension of kakutani's theorem on infinite product measures to the tensor product of semifinite w*-algebras," *Transactions of the American Mathematical Society*, vol. 135, pp. 199–212, 1969.

[BW16] A. Broadbent and E. Wainewright, "Efficient simulation for quantum message authentication," in *International Conference on Information Theoretic Security*, Springer, 2016, pp. 72–91.

[BW88] J. O. Berger and R. L. Wolpert, "The likelihood principle," IMS, 1988.

[BW92] C. H. Bennett and S. J. Wiesner, "Communication via one-and two-particle operators on einstein-podolsky-rosen states," *Physical Review Letters*, vol. 69, no. 20, p. 2881, 1992.

[BŻ17] I. Bengtsson and K. Życzkowski, *Geometry of quantum states: an introduction to quantum entanglement*. Cambridge university press, 2017.

[Cav81] C. M. Caves, "Quantum-mechanical noise in an interferometer," *Physical Review D*, vol. 23, no. 8, p. 1693, 1981.

[CDP09] G. Chiribella, G. M. D'Ariano, and P. Perinotti, "Theoretical framework for quantum networks," *Physical Review A*, vol. 80, no. 2, p. 022 339, 2009.

[CDS05] G. Chiribella, G. D'ariano, and M. Sacchi, "Optimal estimation of group transformations using entanglement," *Physical Review A*, vol. 72, no. 4, p. 042 338, 2005.

[Cha+13] R. Chaves, J. Brask, M. Markiewicz, J. Kołodyński, and A. Acín, "Noisy metrology beyond the standard quantum limit," *Physical Review Letters*, vol. 111, no. 12, p. 120 401, 2013.

[Cha+18] T. Chalopin, C. Bouazza, A. Evrard, V. Makhalov, D. Dreon, J. Dalibard, L. A. Sidorenkov, and S. Nascimbene, "Quantum-enhanced sensing using non-classical spin states of a highly magnetic atom," *Nature Communications*, vol. 9, no. 1, pp. 1–8, 2018.

[Chi+04] G. Chiribella, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, "Covariant quantum measurements that maximize the likelihood," *Physical Review A*, vol. 70, no. 6, p. 062 105, 2004.

[Chi+06] L. Childress, M. G. Dutt, J. Taylor, A. Zibrov, F. Jelezko, J. Wrachtrup, P. Hemmer, and M. Lukin, "Coherent dynamics of coupled electron and nuclear spin qubits in diamond," *Science*, vol. 314, no. 5797, pp. 281–285, 2006.

[CHP12] A. W. Chin, S. F. Huelga, and M. B. Plenio, "Quantum metrology in non-markovian environments," *Physical Review Letters*, vol. 109, no. 23, p. 233 601, 2012.

[CL01] J. Calsamiglia and N. Lütkenhaus, "Maximum efficiency of a linear-optical bell-state analyzer," *Applied Physics B*, vol. 72, no. 1, pp. 67–71, 2001.

[Cle+10] A. A. Clerk, M. H. Devoret, S. M. Girvin, F. Marquardt, and R. J. Schoelkopf, "Introduction to quantum noise, measurement, and amplification," *Reviews of Modern Physics*, vol. 82, no. 2, p. 1155, 2010.

[CMP14] M. Chen, N. C. Menicucci, and O. Pfister, "Experimental realization of multipartite entanglement of 60 modes of a quantum optical frequency comb," *Physical Review Letters*, vol. 112, no. 12, p. 120 505, 2014.

[Cor+15] L. A. Correa, M. Mehboudi, G. Adesso, and A. Sanpera, "Individual quantum probes for optimal thermometry," *Physical Review Letters*, vol. 114, no. 22, p. 220 405, 2015.

[Cox06] D. R. Cox, *Principles of statistical inference*. Cambridge university press, 2006.

[Cra+16] J. Cramer, N. Kalb, M. A. Rol, B. Hensen, M. S. Blok, M. Markham, D. J. Twitchen, R. Hanson, and T. H. Taminiau, "Repeated quantum error correction on a continuously encoded qubit by real-time feedback," *Nature Communications*, vol. 7, no. 1, pp. 1–7, 2016.

[Cra46] H. Cramér, "Mathematical methods of statistics.," *Mathematical methods of statistics.*, 1946.

[Cro+14] P. J. Crowley, A. Datta, M. Barbieri, and I. A. Walmsley, "Tradeoff in simultaneous quantum-limited phase and loss estimation in interferometry," *Physical Review A*, vol. 89, no. 2, p. 023 845, 2014.

[CS08] S. Choi and B. Sundaram, "Bose-einstein condensate as a nonlinear ramsey interferometer operating beyond the heisenberg limit," *Physical Review A*, vol. 77, no. 5, p. 053 613, 2008.

[CS96] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Physical Review A*, vol. 54, no. 2, p. 1098, 1996.

[Dan+09] C. Dankert, R. Cleve, J. Emerson, and E. Livine, "Exact and approximate unitary 2-designs and their application to fidelity estimation," *Physical Review A*, vol. 80, no. 1, p. 012 304, 2009.

[Das+16] T. Das, S. S. Roy, S. Bagchi, A. Misra, A. Sen, U. Sen, *et al.*, "Generalized geometric measure of entanglement for multiparty mixed states," *Physical Review A*, vol. 94, no. 2, p. 022 336, 2016.

[DBE98] R. Derka, V. Buzek, and A. K. Ekert, "Universal algorithm for optimal estimation of quantum states from finite ensembles via realizable generalized measurement," *Physical Review Letters*, vol. 80, no. 8, p. 1571, 1998.

[DCS17] R. Demkowicz-Dobrzański, J. Czajkowski, and P. Sekatski, "Adaptive quantum metrology under general markovian noise," *Physical Review X*, vol. 7, no. 4, p. 041 009, 2017.

[Dem+09] R. Demkowicz-Dobrzanski, U. Dorner, B. Smith, J. Lundeen, W. Wasilewski, K. Banaszek, and I. Walmsley, "Quantum phase estimation with lossy interferometers," *Physical Review A*, vol. 80, no. 1, p. 013 825, 2009.

[Dem11] R. Demkowicz-Dobrzański, "Optimal phase estimation with arbitrary a priori knowledge," *Physical Review A*, vol. 83, no. 6, p. 061 802, 2011.

[Deu85] D. Deutsch, "Quantum theory, the church–turing principle and the universal quantum computer," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 400, no. 1818, pp. 97–117, 1985.

[DG28] C. J. Davisson and L. H. Germer, "Reflection of electrons by a crystal of nickel," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 14, no. 4, p. 317, 1928.

[Die+19] E. Dietsche, A. Larrouy, S. Haroche, J. Raimond, M. Brune, and S. Gleyzes, "High-sensitivity magnetometry with a single atom in a superposition of two circular rydberg states," *Nature Physics*, vol. 15, no. 4, pp. 326–329, 2019.

[DJK15] R. Demkowicz-Dobrzański, M. Jarzyna, and J. Kołodyński, "Quantum limits in optical interferometry," *Progress in Optics*, vol. 60, pp. 345–435, 2015.

[DKG12] R. Demkowicz-Dobrzański, J. Kołodyński, and M. Guţă, "The elusive heisenberg limit in quantum-enhanced metrology," *Nature Communications*, vol. 3, no. 1, pp. 1–8, 2012.

[DM03] J. P. Dowling and G. J. Milburn, "Quantum technology: The second quantum revolution," *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 361, no. 1809, pp. 1655–1674, 2003.

[DMN13] S. J. Devitt, W. J. Munro, and K. Nemoto, "Quantum error correction for beginners," *Reports on Progress in Physics*, vol. 76, no. 7, p. 076 001, 2013.

[Dor12] U. Dorner, "Quantum frequency estimation with trapped ions and atoms," *New Journal of Physics*, vol. 14, no. 4, p. 043 011, 2012.

[Dow08] J. P. Dowling, "Quantum optical metrology–the lowdown on high-n00n states," *Contemporary Physics*, vol. 49, no. 2, pp. 125–143, 2008.

[DPD19] P. Djorwe, Y. Pennec, and B. Djafari-Rouhani, "Exceptional point enhances sensitivity of optomechanical mass sensors," *Physical Review Applied*, vol. 12, no. 2, p. 024 002, 2019.

[DRC17] C. L. Degen, F. Reinhard, and P. Cappellaro, "Quantum sensing," *Reviews of Modern Physics*, vol. 89, no. 3, p. 035 002, 2017.

[DS18] A. De Pasquale and T. M. Stace, "Quantum thermometry," *arXiv preprint arXiv:1807.05762*, 2018.

[DSM16] K. E. Dorfman, F. Schlawin, and S. Mukamel, "Nonlinear optical signals and spectroscopy with quantum light," *Reviews of Modern Physics*, vol. 88, no. 4, p. 045 008, 2016.

[Dür+14] W. Dür, M. Skotiniotis, F. Froewis, and B. Kraus, "Improved quantum metrology using quantum error correction," *Physical Review Letters*, vol. 112, no. 8, p. 080 801, 2014.

[Dut+07] M. G. Dutt, L. Childress, L. Jiang, E. Togan, J. Maze, F. Jelezko, A. Zibrov, P. Hemmer, and M. Lukin, "Quantum register based on individual electronic and nuclear spin qubits in diamond," *Science*, vol. 316, no. 5829, pp. 1312–1316, 2007.

[EdMD11a] B. Escher, R. de Matos Filho, and L. Davidovich, "Quantum metrology for noisy systems," *Brazilian Journal of Physics*, vol. 41, no. 4, pp. 229–247, 2011.

[EdMD11b] B. Escher, R. de Matos Filho, and L. Davidovich, "General framework for estimating the ultimate precision limit in noisy quantum-enhanced metrology," *Nature Physics*, vol. 7, no. 5, pp. 406–411, 2011.

[Eld+18] Z. Eldredge, M. Foss-Feig, J. A. Gross, S. L. Rolston, and A. V. Gorshkov, "Optimal and secure measurement protocols for quantum sensor networks," *Physical Review A*, vol. 97, no. 4, p. 042 337, 2018.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Physical Review*, vol. 47, no. 10, p. 777, 1935.

[Fac+10] P. Facchi, R. Kulkarni, V. Man'ko, G. Marmo, E. Sudarshan, and F. Ventriglia, "Classical and quantum fisher information in the geometrical formulation of quantum mechanics," *Physics Letters A*, vol. 374, no. 48, pp. 4801–4803, 2010.

[Fac+16] A. Facon, E.-K. Dietsche, D. Grosso, S. Haroche, J.-M. Raimond, M. Brune, and S. Gleyzes, "A sensitive electrometer based on a rydberg atom in a schrödinger-cat state," *Nature*, vol. 535, no. 7611, pp. 262–265, 2016.

[Fey82] R. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, no. 6, 1982.

[FGV15] Y. Fujiwara, A. Gruner, and P. Vandendriessche, "High-rate quantum low-density parity-check codes assisted by reliable qubits," *IEEE Transactions on Information Theory*, vol. 61, no. 4, pp. 1860–1878, 2015.

[Fis25] R. A. Fisher, "Theory of statistical estimation," in *Mathematical proceedings of the Cambridge philosophical society*, Cambridge University Press, vol. 22, 1925, pp. 700–725.

[FK17] J. F. Fitzsimons and E. Kashefi, "Unconditionally verifiable blind quantum computation," *Physical Review A*, vol. 96, no. 1, p. 012 303, 2017.

[Fra+21] G. Frascella, S. Agne, F. Y. Khalili, and M. V. Chekhova, "Overcoming detection loss and noise in squeezing-based optical sensing," *npj Quantum Information*, vol. 7, no. 1, pp. 1–6, 2021.

[Fri+17] N. Friis, D. Orsucci, M. Skotiniotis, P. Sekatski, V. Dunjko, H. J. Briegel, and W. Dür, "Flexible resources for quantum metrology," *New Journal of Physics*, vol. 19, no. 6, p. 063 044, 2017.

[Fuj01] A. Fujiwara, "Estimation of su (2) operation and dense coding: An information geometric approach," *Physical Review A*, vol. 65, no. 1, p. 012 316, 2001.

[Fuj06] ——, "Strong consistency and asymptotic efficiency for adaptive quantum estimation problems," *Journal of Physics A: Mathematical and General*, vol. 39, no. 40, p. 12 489, 2006.

[FV99] C. A. Fuchs and J. Van De Graaf, "Cryptographic distinguishability measures for quantum-mechanical states," *IEEE Transactions on Information Theory*, vol. 45, no. 4, pp. 1216–1227, 1999.

[Gar91] C. W. Gardiner, "Quantum noise," *Springer series in synergetics*, 1991.

[Ge+18] W. Ge, K. Jacobs, Z. Eldredge, A. V. Gorshkov, and M. Foss-Feig, "Distributed quantum metrology with linear networks and separable inputs," *Physical Review Letters*, vol. 121, no. 4, p. 043 604, 2018.

[Gen16] M. Genovese, "Real applications of quantum imaging," *Journal of Optics*, vol. 18, no. 7, p. 073 002, 2016.

[GG13] R. D. Gill and M. I. Guţă, "On asymptotic quantum statistical inference," in *From Probability to Statistics and Back: High-Dimensional Models and Processes–A Festschrift in Honor of Jon A. Wellner*, Institute of Mathematical Statistics, 2013, pp. 105–127.

[GKK19] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, "Verification of quantum computation: An overview of existing approaches," *Theory of Computing Systems*, vol. 63, no. 4, pp. 715–808, 2019.

[GKM05] J. Grabowski, M. Kuś, and G. Marmo, "Geometry of quantum systems: Density states and entanglement," *Journal of Physics A: Mathematical and General*, vol. 38, no. 47, p. 10 217, 2005.

[GLM01] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum-enhanced positioning and clock synchronization," *Nature*, vol. 412, no. 6845, pp. 417–419, 2001.

[GLM04] ——, "Quantum-enhanced measurements: Beating the standard quantum limit," *Science*, vol. 306, no. 5700, pp. 1330–1336, 2004.

[GLM06] ——, "Quantum metrology," *Physical Review Letters*, vol. 96, no. 1, p. 010 401, 2006.

[GLM11] ——, "Advances in quantum metrology," *Nature photonics*, vol. 5, no. 4, pp. 222–229, 2011.

[GM05] R. D. Gill and S. Massar, "State estimation for large ensembles," in *Asymptotic Theory Of Quantum Statistical Inference: Selected Papers*, World Scientific, 2005, pp. 178–214.

[GM13] S. Gammelmark and K. Mølmer, "Bayesian parameter inference from continuously monitored quantum systems," *Physical Review A*, vol. 87, no. 3, p. 032 115, 2013.

[GMC17] H. J. García, I. L. Markov, and A. W. Cross, "On the geometry of stabilizer states," *arXiv preprint arXiv:1711.07848*, 2017.

[Gon+19] M. Gong, M.-C. Chen, Y. Zheng, S. Wang, C. Zha, H. Deng, Z. Yan, H. Rong, Y. Wu, S. Li, *et al.*, "Genuine 12-qubit entanglement on a superconducting quantum processor," *Physical Review Letters*, vol. 122, no. 11, p. 110 501, 2019.

[Got96] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum hamming bound," *Physical Review A*, vol. 54, no. 3, p. 1862, 1996.

[Got97] ——, *Stabilizer codes and quantum error correction*. California Institute of Technology, 1997.

[Got98] ——, "The heisenberg representation of quantum computers," *arXiv preprint quant-ph/9807006*, 1998.

[Gro12] C. Gross, "Spin squeezing, entanglement and quantum metrology with bose–einstein condensates," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 45, no. 10, p. 103 001, 2012.

[GS18] D. J. Griffiths and D. F. Schroeter, *Introduction to quantum mechanics*. Cambridge University Press, 2018.

[GS22] W. Gerlach and O. Stern, "Der experimentelle nachweis der richtungsquantelung im magnetfeld," *Zeitschrift für Physik*, vol. 9, no. 1, pp. 349–352, 1922.

[Gu+19] X. Gu, M. Erhard, A. Zeilinger, and M. Krenn, "Quantum experiments and graphs ii: Quantum interference, computation, and state generation," *Proceedings of the National Academy of Sciences*, vol. 116, no. 10, pp. 4147–4155, 2019.

[Guo+20] X. Guo, C. R. Breum, J. Borregaard, S. Izumi, M. V. Larsen, T. Gehring, M. Christandl, J. S. Neergaard-Nielsen, and U. L. Andersen, "Distributed quantum sensing in a continuous-variable entangled network," *Nature Physics*, vol. 16, no. 3, pp. 281–284, 2020.

[Haa+16] J. F. Haase, A. Smirne, S. Huelga, J. Kołodynski, and R. Demkowicz-Dobrzanski, "Precision limits in quantum metrology with open quantum systems," *Quantum Measurements and Quantum Metrology*, vol. 5, no. 1, pp. 13–39, 2016.

[Hay+04] P. Hayden, D. Leung, P. W. Shor, and A. Winter, "Randomizing quantum states: Constructions and applications," *Communications in Mathematical Physics*, vol. 250, no. 2, pp. 371–391, 2004.

[Hay05] M. Hayashi, *Asymptotic theory of quantum statistical inference: selected papers*. World Scientific, 2005.

[HB93] M. Holland and K. Burnett, "Interferometric detection of optical phase shifts at the heisenberg limit," *Physical Review Letters*, vol. 71, no. 9, p. 1355, 1993.

[HBD09] M.-H. Hsieh, T. A. Brun, and I. Devetak, "Entanglement-assisted quantum quasicyclic low-density parity-check codes," *Physical Review A*, vol. 79, no. 3, p. 032 340, 2009.

[HEB04] M. Hein, J. Eisert, and H. J. Briegel, "Multiparty entanglement in graph states," *Physical Review A*, vol. 69, no. 6, p. 062 311, 2004.

[Hei+06] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Nest, and H.-J. Briegel, "Entanglement in graph states and its applications," *arXiv preprint quant-ph/0602096*, 2006.

[Hel67] C. W. Helstrom, "Minimum mean-squared error of estimates in quantum statistics," *Physics letters A*, vol. 25, no. 2, pp. 101–102, 1967.

[Hel68] C. Helstrom, "The minimum variance of estimates in quantum signal detection," *IEEE Transactions on Information Theory*, vol. 14, no. 2, pp. 234–242, 1968.

[Hel69] C. W. Helstrom, "Quantum detection and estimation theory," *Journal of Statistical Physics*, vol. 1, no. 2, pp. 231–252, 1969.

[Her+15] D. A. Herrera-Martí, T. Gefen, D. Aharonov, N. Katz, and A. Retzker, "Quantum error-correction-enhanced magnetometer overcoming the limit imposed by relaxation," *Physical Review Letters*, vol. 115, no. 20, p. 200 501, 2015.

[HGS10] P. Hyllus, O. Gühne, and A. Smerzi, "Not all pure entangled states are useful for sub-shot-noise interferometry," *Physical Review A*, vol. 82, no. 1, p. 012 337, 2010.

[HK69] K.-E. Hellwig and K. Kraus, "Pure operations and measurements," *Communications in Mathematical Physics*, vol. 11, no. 3, pp. 214–220, 1969.

[HK74] C. Helstrom and R. Kennedy, "Noncommuting observables in quantum detection and estimation theory," *IEEE Transactions on Information Theory*, vol. 20, no. 1, pp. 16–24, 1974.

[HMM19] Z. Huang, C. Macchiavello, and L. Maccone, "Cryptographic quantum metrology," *Physical Review A*, vol. 99, no. 2, p. 022 314, 2019.

[Hol73] A. S. Holevo, "Statistical decision theory for quantum systems," *Journal of Multivariate Analysis*, vol. 3, no. 4, pp. 337–394, 1973.

[Hol82] ——, *Probabilistic and statistical aspects of quantum theory*. Holland Publishing Company, 1982.

[HPE19] F. Hahn, A. Pappa, and J. Eisert, "Quantum network routing and local complementation," *npj Quantum Information*, vol. 5, no. 1, pp. 1–7, 2019.

[Hua+19] C.-Y. Huang, N. Lambert, C.-M. Li, Y.-T. Lu, and F. Nori, "Securing quantum networking tasks with multipartite einstein-podolsky-rosen steering," *Physical Review A*, vol. 99, no. 1, p. 012 302, 2019.

[Hue+97] S. F. Huelga, C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio, and J. I. Cirac, "Improvement of frequency standards with quantum entanglement," *Physical Review Letters*, vol. 79, no. 20, p. 3865, 1997.

[Hum+13] P. C. Humphreys, M. Barbieri, A. Datta, and I. A. Walmsley, "Quantum enhanced multiple phase estimation," *Physical Review Letters*, vol. 111, no. 7, p. 070 403, 2013.

[Jac14] K. Jacobs, *Quantum measurement theory and its applications*. Cambridge University Press, 2014.

[JCH14] J. Jeske, J. H. Cole, and S. F. Huelga, "Quantum metrology subject to spatially correlated markovian noise: Restoring the heisenberg limit," *New Journal of Physics*, vol. 16, no. 7, p. 073 039, 2014.

[JD15] M. Jarzyna and R. Demkowicz-Dobrzański, "True precision limits in quantum metrology," *New Journal of Physics*, vol. 17, no. 1, p. 013 010, 2015.

[JLM11] T. Jahnke, S. Lanéry, and G. Mahler, "Operational approach to fluctuations of thermodynamic variables in finite quantum systems," *Physical Review E*, vol. 83, no. 1, p. 011 109, 2011.

[Kac+10] M. Kacprowicz, R. Demkowicz-Dobrzański, W. Wasilewski, K. Banaszek, and I. Walmsley, "Experimental quantum-enhanced estimation of a lossy phase shift," *Nature Photonics*, vol. 4, no. 6, pp. 357–360, 2010.

[Kas+21] H. Kasai, Y. Takeuchi, H. Hakoshima, Y. Matsuzaki, and Y. Tokura, "Anonymous quantum sensing," *arXiv preprint arXiv:2105.05585*, 2021.

[Kay93] S. M. Kay, *Fundamentals of statistical signal processing: estimation theory*. Prentice-Hall, Inc., 1993.

[KD10] J. Kołodyński and R. Demkowicz-Dobrzański, "Phase estimation without a priori phase knowledge in the presence of loss," *Physical Review A*, vol. 82, no. 5, p. 053 804, 2010.

[KD13] ——, "Efficient tools for quantum metrology with uncorrelated noise," *New Journal of Physics*, vol. 15, no. 7, p. 073 043, 2013.

[KD21] A. Kubica and R. Demkowicz-Dobrzański, "Using quantum metrological bounds in quantum error correction: A simple proof of the approximate eastin-knill theorem," *Physical Review Letters*, vol. 126, no. 15, p. 150 503, 2021.

[Kes+14] E. M. Kessler, I. Lovchinsky, A. O. Sushkov, and M. D. Lukin, "Quantum error correction for metrology," *Physical Review Letters*, vol. 112, no. 15, p. 150 802, 2014.

[Kim08] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, 2008.

[Kir+11] M. Kira, S. W. Koch, R. P. Smith, A. E. Hunter, and S. T. Cundiff, "Quantum spectroscopy with schrödinger-cat states," *Nature Physics*, vol. 7, no. 10, pp. 799–804, 2011.

[Kit95] A. Y. Kitaev, "Quantum measurements and the abelian stabilizer problem," *arXiv preprint quant-ph/9511026*, 1995.

[Kit97] A. Y. Kitaev, "Quantum computations: Algorithms and error correction," *Uspekhi Matematicheskikh Nauk*, vol. 52, no. 6, pp. 53–112, 1997.

[Koc+20] B. Koczor, S. Endo, T. Jones, Y. Matsuzaki, and S. C. Benjamin, "Variational-state quantum metrology," *New Journal of Physics*, vol. 22, no. 8, p. 083 038, 2020.

[Kol14] J. Kolodynski, "Precision bounds in noisy quantum metrology," *arXiv preprint arXiv:1409.0535*, 2014.

[Kol20] A. R. Kolovsky, "Quantum entanglement and the born-markov approximation for an open quantum system," *Physical Review E*, vol. 101, no. 6, p. 062 116, 2020.

[Kóm+14] P. Kómár, E. Kessler, M. Bishof, L. Jiang, A. Sørensen, J. Ye, and M. Lukin, "A quantum network of clocks," *Nature Physics*, vol. 10, no. 8, pp. 582–587, 2014.

[Kóm+16] P. Kómár, T. Topcu, E. Kessler, A. Derevianko, V. Vuletić, J. Ye, and M. D. Lukin, "Quantum network of atom clocks: A possible implementation with neutral atoms," *Physical Review Letters*, vol. 117, no. 6, p. 060 506, 2016.

[Kri+18] M. Kritsotakis, S. S. Szigeti, J. A. Dunningham, and S. A. Haine, "Optimal matter-wave gravimetry," *Physical Review A*, vol. 98, no. 2, p. 023 629, 2018.

[KSD11] S. Knysh, V. N. Smelyanskiy, and G. A. Durkin, "Scaling laws for precision in quantum interferometry and the bifurcation landscape of the optimal state," *Physical Review A*, vol. 83, no. 2, p. 021 804, 2011.

[Ku+66] H. H. Ku *et al.*, "Notes on the use of propagation of error formulas," *Journal of Research of the National Bureau of Standards*, vol. 70, no. 4, pp. 263–273, 1966.

[Kuc+13] G. Kucsko, P. C. Maurer, N. Y. Yao, M. Kubo, H. J. Noh, P. K. Lo, H. Park, and M. D. Lukin, "Nanometre-scale thermometry in a living cell," *Nature*, vol. 500, no. 7460, pp. 54–58, 2013.

[Kul97] S. Kullback, *Information theory and statistics*. Courier Corporation, 1997.

[Laf+96] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," *Physical Review Letters*, vol. 77, no. 1, p. 198, 1996.

[Lan+13] B. Lanyon, P. Jurcevic, M. Zwerger, C. Hempel, E. Martinez, W. Dür, H. Briegel, R. Blatt, and C. F. Roos, "Measurement-based quantum computation with trapped ions," *Physical Review Letters*, vol. 111, no. 21, p. 210 501, 2013.

[Lay+19] D. Layden, S. Zhou, P. Cappellaro, and L. Jiang, "Ancilla-free quantum error correction codes for quantum metrology," *Physical Review Letters*, vol. 122, no. 4, p. 040 502, 2019.

[LC18] D. Layden and P. Cappellaro, "Spatial noise filtering through error correction for quantum sensing," *npj Quantum Information*, vol. 4, no. 1, pp. 1–6, 2018.

[Lee+09] T.-W. Lee, S. D. Huver, H. Lee, L. Kaplan, S. B. McCracken, C. Min, D. B. Uskov, C. F. Wildfeuer, G. Veronis, and J. P. Dowling, "Optimization of quantum interferometric metrological sensors in the presence of photon loss," *Physical Review A*, vol. 80, no. 6, p. 063 803, 2009.

[Lei+04] D. Leibfried, M. D. Barrett, T. Schaetz, J. Britton, J. Chiaverini, W. M. Itano, J. D. Jost, C. Langer, and D. J. Wineland, "Toward heisenberg-limited spectroscopy with multiparticle entangled states," *Science*, vol. 304, no. 5676, pp. 1476–1478, 2004.

[Leu+97] D. W. Leung, M. A. Nielsen, I. L. Chuang, and Y. Yamamoto, "Approximate quantum error correction can lead to better codes," *Physical Review A*, vol. 56, no. 4, p. 2567, 1997.

[LGB02] L. Lugiato, A. Gatti, and E. Brambilla, "Quantum imaging," *arXiv preprint quant-ph/0203046*, 2002.

[Li+18] Y. Li, L. Pezzè, M. Gessner, Z. Ren, W. Li, and A. Smerzi, "Frequentist and bayesian quantum phase estimation," *Entropy*, vol. 20, no. 9, p. 628, 2018.

[Lia+17] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[LIG17] LIGO. (2017). "Ligo: Facts," [Online]. Available: https://www.ligo.caltech.edu/page/facts (visited on 08/03/2021).

[Lin76] G. Lindblad, "On the generators of quantum dynamical semigroups," *Communications in Mathematical Physics*, vol. 48, no. 2, pp. 119–130, 1976.

[Liu+19] Y.-C. Liu, X.-D. Yu, J. Shang, H. Zhu, and X. Zhang, "Efficient verification of dicke states," *Physical Review Applied*, vol. 12, no. 4, p. 044 020, 2019.

[LL15] C. Lupo and S. Lloyd, "Quantum data locking for high-rate private communication," *New Journal of Physics*, vol. 17, no. 3, p. 033 022, 2015.

[Lu+07] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, and J.-W. Pan, "Experimental entanglement of six photons in graph states," *Nature Physics*, vol. 3, no. 2, pp. 91–95, 2007.

[Lud+15] A. D. Ludlow, M. M. Boyd, J. Ye, E. Peik, and P. O. Schmidt, "Optical atomic clocks," *Reviews of Modern Physics*, vol. 87, no. 2, p. 637, 2015.

[Lui04] A. Luis, "Nonlinear transformations and the heisenberg limit," *Physics Letters A*, vol. 329, no. 1-2, pp. 8–13, 2004.

[Luo00] S. Luo, "Quantum fisher information and uncertainty relations," *Letters in Mathematical Physics*, vol. 53, no. 3, pp. 243–251, 2000.

[Lvo15] A. I. Lvovsky, "Squeezed light," *Photonics: Scientific Foundations, Technology and Applications*, vol. 1, pp. 121–163, 2015.

[LYO15] X.-M. Lu, S. Yu, and C. Oh, "Robust quantum metrological schemes based on protection of quantum fisher information," *Nature Communications*, vol. 6, no. 1, pp. 1–7, 2015.

[Mat+16] J. C. Matthews, X.-Q. Zhou, H. Cable, P. J. Shadbolt, D. J. Saunders, G. A. Durkin, G. J. Pryde, and J. L. O'Brien, "Towards practical quantum metrology with photon counting," *npj Quantum Information*, vol. 2, no. 1, pp. 1–7, 2016.

[Mat02] K. Matsumoto, "A new approach to the cramér-rao-type bound of the pure-state model," *Journal of Physics A: Mathematical and General*, vol. 35, no. 13, p. 3111, 2002.

[MB17] Y. Matsuzaki and S. Benjamin, "Magnetic-field sensing with quantum error detection under the effect of energy relaxation," *Physical Review A*, vol. 95, no. 3, p. 032 303, 2017.

[MBE21] J. J. Meyer, J. Borregaard, and J. Eisert, "A variational toolbox for quantum multi-parameter estimation," *npj Quantum Information*, vol. 7, no. 1, pp. 1–5, 2021.

[Mey+01] V. Meyer, M. Rowe, D. Kielpinski, C. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, "Experimental demonstration of entanglement-enhanced rotation angle estimation using trapped ions," *Physical Review Letters*, vol. 86, no. 26, p. 5870, 2001.

[Mez+18] R. Mezher, J. Ghalbouni, J. Dgheim, and D. Markham, "Efficient quantum pseudorandomness with simple graph states," *Physical Review A*, vol. 97, no. 2, p. 022 333, 2018.

[MFD14] K. Macieszczak, M. Fraas, and R. Demkowicz-Dobrzański, "Bayesian quantum frequency estimation in presence of collective dephasing," *New Journal of Physics*, vol. 16, no. 11, p. 113 002, 2014.

[MK20] D. Markham and A. Krause, "A simple protocol for certifying graph states and applications in quantum networks," *Cryptography*, vol. 4, no. 1, p. 3, 2020.

[MMG19] C. Meignant, D. Markham, and F. Grosshans, "Distributing graph states over arbitrary quantum networks," *Physical Review A*, vol. 100, no. 5, p. 052 333, 2019.

[MO18] J. Mejía-Salazar and O. N. Oliveira Jr, "Plasmonic biosensing: Focus review," *Chemical Reviews*, vol. 118, no. 20, pp. 10 617–10 625, 2018.

[Mor14] T. Morimae, "Verification for measurement-only blind quantum computing," *Physical Review A*, vol. 89, no. 6, p. 060 302, 2014.

[MR11] U. Maurer and R. Renner, "Abstract cryptography," in *In Innovations in Computer Science*, Citeseer, 2011.

[MS08] D. Markham and B. C. Sanders, "Graph states for quantum secret sharing," *Physical Review A*, vol. 78, no. 4, p. 042 309, 2008.

[MSC19] M. Mehboudi, A. Sanpera, and L. A. Correa, "Thermometry in the quantum regime: Recent theoretical progress," *Journal of Physics A: Mathematical and Theoretical*, vol. 52, no. 30, p. 303 001, 2019.

[MY98] D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus," in *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)*, IEEE, 1998, pp. 503–509.

[Nag+07] T. Nagata, R. Okamoto, J. L. O'brien, K. Sasaki, and S. Takeuchi, "Beating the standard quantum limit with four-entangled photons," *Science*, vol. 316, no. 5825, pp. 726–729, 2007.

[NC02] M. A. Nielsen and I. Chuang, *Quantum computation and quantum information*, 2002.

[Neu+13] P. Neumann, I. Jakobi, F. Dolde, C. Burk, R. Reuter, G. Waldherr, J. Honert, T. Wolf, A. Brunner, J. H. Shim, *et al.*, "High-precision nanoscale temperature sensing using single defects in diamond," *Nano Letters*, vol. 13, no. 6, pp. 2738–2742, 2013.

[Nic+18] R. Nichols, P. Liuzzo-Scorpo, P. A. Knott, and G. Adesso, "Multi-parameter gaussian quantum metrology," *Physical Review A*, vol. 98, no. 1, p. 012 114, 2018.

[Nie13] F. Nielsen, "Cramér-rao lower bound and information geometry," in *Connected at Infinity II*, Springer, 2013, pp. 18–37.

[NWD14] P. Niemann, R. Wille, and R. Drechsler, "Efficient synthesis of quantum circuits implementing clifford group operations," in *2014 19th Asia and South Pacific Design Automation Conference (ASP-DAC)*, IEEE, 2014, pp. 483–488.

[Ofe+16] N. Ofek, A. Petrenko, R. Heeres, P. Reinhold, Z. Leghtas, B. Vlastakis, Y. Liu, L. Frunzio, S. Girvin, L. Jiang, *et al.*, "Extending the lifetime of a quantum bit with error correction in superconducting circuits," *Nature*, vol. 536, no. 7617, pp. 441–445, 2016.

[OH10] T. Ono and H. F. Hofmann, "Effects of photon losses on phase estimation near the heisenberg limit using coherent light and squeezed vacuum," *Physical Review A*, vol. 81, no. 3, p. 033 819, 2010.

[Oka+08] R. Okamoto, H. F. Hofmann, T. Nagata, J. L. O'Brien, K. Sasaki, and S. Takeuchi, "Beating the standard quantum limit: Phase supersensitivity of n-photon interferometers," *New Journal of Physics*, vol. 10, no. 7, p. 073 033, 2008.

[Oka+20] H. Okane, H. Hakoshima, Y. Takeuchi, Y. Seki, and Y. Matsuzaki, "Quantum remote sensing under the effect of dephasing," *arXiv preprint arXiv:2007.15903*, 2020.

[OSM19] Y. Ouyang, N. Shettell, and D. Markham, "Robust quantum metrology with explicit symmetric states," *arXiv preprint arXiv:1908.02378*, 2019.

[Osz+16] M. Oszmaniec, R. Augusiak, C. Gogolin, J. Kołodyński, A. Acin, and M. Lewenstein, "Random bosonic states for robust quantum metrology," *Physical Review X*, vol. 6, no. 4, p. 041 044, 2016.

[OTT19] T. E. O'Brien, B. Tarasinski, and B. M. Terhal, "Quantum phase estimation of multiple eigenvalues for small-scale (noisy) experiments," *New Journal of Physics*, vol. 21, no. 2, p. 023 022, 2019.

[Ou12] Z. Ou, "Enhancement of the phase-measurement sensitivity beyond the standard quantum limit by a nonlinear interferometer," *Physical Review A*, vol. 85, no. 2, p. 023 815, 2012.

[Ouy14] Y. Ouyang, "Permutation-invariant quantum codes," *Physical Review A*, vol. 90, no. 6, p. 062 317, 2014.

[Pap+12] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, "Multipartite entanglement verification resistant against dishonest parties," *Physical Review Letters*, vol. 108, no. 26, p. 260 502, 2012.

[Pap+14] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, "Experimental plug and play quantum coin flipping," *Nature Communications*, vol. 5, no. 1, pp. 1–8, 2014.

[Par09] M. G. Paris, "Quantum estimation for quantum technology," *International Journal of Quantum Information*, vol. 7, no. supp01, pp. 125–137, 2009.

[Ped+19] E. Pednault, J. Gunnels, D. Maslov, and J. Gambetta, *On quantum supremacy*, 2019.

[Peñ+12] Á. B. Peña, B. Kemper, M. Woerdemann, A. Vollmer, S. Ketelhut, G. von Bally, and C. Denz, "Optical tweezers induced photodamage in living cells quantified with digital holographic phase microscopy," in *Biophotonics: Photonic Solutions for Better Health Care III*, International Society for Optics and Photonics, vol. 8427, 2012, 84270A.

[Pez+18] L. Pezze, A. Smerzi, M. K. Oberthaler, R. Schmied, and P. Treutlein, "Quantum metrology with nonclassical states of atomic ensembles," *Reviews of Modern Physics*, vol. 90, no. 3, p. 035 005, 2018.

[PH16] M. B. Plenio and S. F. Huelga, "Sensing in the presence of an observed environment," *Physical Review A*, vol. 93, no. 3, p. 032 123, 2016.

[Phi84] G. D. Phillies, "The polythermal ensemble: A rigorous interpretation of temperature fluctuations in statistical mechanics," *American Journal of Physics*, vol. 52, no. 7, pp. 629–632, 1984.

[Pir+18] S. Pirandola, B. R. Bardhan, T. Gehring, C. Weedbrook, and S. Lloyd, "Advances in photonic quantum sensing," *Nature Photonics*, vol. 12, no. 12, pp. 724–733, 2018.

[Pir+20] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, *et al.*, "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[PJ17] S. Pang and A. N. Jordan, "Optimal adaptive control for quantum metrology with time-dependent hamiltonians," *Nature Communications*, vol. 8, no. 1, pp. 1–9, 2017.

[PKD18] T. J. Proctor, P. A. Knott, and J. A. Dunningham, "Multiparameter estimation in networked quantum sensors," *Physical Review Letters*, vol. 120, no. 8, p. 080 501, 2018.

[PLM18] S. Pallister, N. Linden, and A. Montanaro, "Optimal verification of entangled states with local measurements," *Physical Review Letters*, vol. 120, no. 17, p. 170 502, 2018.

[Poo13] H. V. Poor, *An introduction to signal detection and estimation*. Springer Science & Business Media, 2013.

[PR04] H. Pollatsek and M. B. Ruskai, "Permutationally invariant codes for quantum error correction," *Linear Algebra and its Applications*, vol. 392, pp. 255–288, 2004.

[Pre12] J. Preskill, "Quantum computing and the entanglement frontier," *arXiv preprint arXiv:1203.5813*, 2012.

[Pre18] ——, "Quantum computing in the nisq era and beyond," *Quantum*, vol. 2, p. 79, 2018.

[Pre98] ——, "Fault-tolerant quantum computation," in *Introduction to quantum computation and information*, World Scientific, 1998, pp. 213–269.

[PS09] L. Pezzé and A. Smerzi, "Entanglement, nonlinear dynamics, and the heisenberg limit," *Physical Review Letters*, vol. 102, no. 10, p. 100 401, 2009.

[PS96] D. Petz and C. Sudár, "Geometries of quantum states," *Journal of Mathematical Physics*, vol. 37, no. 6, pp. 2662–2673, 1996.

[PWD18] A. Pirker, J. Wallnöfer, and W. Dür, "Modular architectures for quantum networks," *New Journal of Physics*, vol. 20, no. 5, p. 053 054, 2018.

[PZ98] J. P. Paz and W. H. Zurek, "Continuous error correction," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 454, no. 1969, pp. 355–364, 1998.

[Qia+12] Y. Qian, Z. Shen, G. He, and G. Zeng, "Quantum-cryptography network via continuous-variable graph states," *Physical Review A*, vol. 86, no. 5, p. 052 333, 2012.

[Qia+19] K. Qian, Z. Eldredge, W. Ge, G. Pagano, C. Monroe, J. V. Porto, and A. V. Gorshkov, "Heisenberg-scaling measurement protocol for analytic functions with quantum sensor networks," *Physical Review A*, vol. 100, no. 4, p. 042 304, 2019.

[Qva+18] S. Qvarfort, A. Serafini, P. F. Barker, and S. Bose, "Gravimetry through non-linear optomechanics," *Nature Communications*, vol. 9, no. 1, pp. 1–11, 2018.

[Rad45] C. Radhakrishna Rao, "Information and accuracy attainable in the estimation of statistical parameters," *Bulletin of the Calcutta Mathematical Society*, vol. 37, no. 3, pp. 81–91, 1945.

[Raz+19] L. Razzoli, L. Ghirardi, I. Siloi, P. Bordone, and M. G. Paris, "Lattice quantum magnetometry," *Physical Review A*, vol. 99, no. 6, p. 062 330, 2019.

[RB01] R. Raussendorf and H. J. Briegel, "A one-way quantum computer," *Physical Review Letters*, vol. 86, no. 22, p. 5188, 2001.

[RBB03] R. Raussendorf, D. E. Browne, and H. J. Briegel, "Measurement-based quantum computation on cluster states," *Physical Review A*, vol. 68, no. 2, p. 022 312, 2003.

[RBE19] A. Russo, E. Barnes, and S. E. Economou, "Generation of arbitrary all-photonic graph states from quantum emitters," *New Journal of Physics*, vol. 21, no. 5, p. 055 002, 2019.

[RD20] J. Rubio and J. Dunningham, "Bayesian multiparameter quantum metrology with limited data," *Physical Review A*, vol. 101, no. 3, p. 032 114, 2020.

[Ree+12] M. D. Reed, L. DiCarlo, S. E. Nigg, L. Sun, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf, "Realization of three-qubit quantum error correction with superconducting circuits," *Nature*, vol. 482, no. 7385, pp. 382–385, 2012.

[RH12] A. Rivas and S. F. Huelga, *Open quantum systems*. Springer, 2012, vol. 10.

[RH96] J. Raimond and S. Haroche, "Quantum computing: Dream or nightmare," *Physics Today*, vol. 49, no. 8, pp. 51–52, 1996.

[Ric06] J. A. Rice, *Mathematical statistics and data analysis*. Cengage Learning, 2006.

[RJ09] M. Rosenkranz and D. Jaksch, "Parameter estimation with cluster states," *Physical Review A*, vol. 79, no. 2, p. 022 103, 2009.

[RJD16] S. Ragy, M. Jarzyna, and R. Demkowicz-Dobrzański, "Compatibility in multiparameter quantum metrology," *Physical Review A*, vol. 94, no. 5, p. 052 108, 2016.

[RKD18] J. Rubio, P. Knott, and J. Dunningham, "Non-asymptotic analysis of quantum metrology protocols beyond the cramér–rao bound," *Journal of Physics Communications*, vol. 2, no. 1, p. 015 027, 2018.

[Rob29] H. P. Robertson, "The uncertainty principle," *Physical Review*, vol. 34, no. 1, p. 163, 1929.

[Rof+18] J. Roffe, D. Headley, N. Chancellor, D. Horsman, and V. Kendon, "Protecting quantum memories using coherent parity check codes," *Quantum Science and Technology*, vol. 3, no. 3, p. 035 010, 2018.

[Ron+11] X. Rong, P. Huang, X. Kong, X. Xu, F. Shi, Y. Wang, and J. Du, "Enhanced phase estimation by implementing dynamical decoupling in a multi-pass quantum metrology protocol," *EPL (Europhysics Letters)*, vol. 95, no. 6, p. 60 005, 2011.

[Ros+20] M. A. Rossi, F. Albarelli, D. Tamascelli, and M. G. Genoni, "Noisy quantum metrology enhanced by continuous nondemolition measurement," *Physical Review Letters*, vol. 125, no. 20, p. 200 505, 2020.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[Rub+20] J. Rubio, P. A. Knott, T. J. Proctor, and J. A. Dunningham, "Quantum sensing networks for the estimation of linear functions," *Journal of Physics A: Mathematical and Theoretical*, vol. 53, no. 34, p. 344 001, 2020.

[SÁ16] D. Suter and G. A. Álvarez, "Colloquium: Protecting quantum information against environmental noise," *Reviews of Modern Physics*, vol. 88, no. 4, p. 041 001, 2016.

[SÁS12] A. M. Souza, G. A. Álvarez, and D. Suter, "Robust dynamical decoupling," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 370, no. 1976, pp. 4748–4769, 2012.

[SBD16] M. Szczykulska, T. Baumgratz, and A. Datta, "Multi-parameter quantum metrology," *Advances in Physics: X*, vol. 1, no. 4, pp. 621–639, 2016.

[SC07] A. Shaji and C. M. Caves, "Qubit metrology and decoherence," *Physical Review A*, vol. 76, no. 3, p. 032 111, 2007.

[Sch+11] P. Schindler, J. T. Barreiro, T. Monz, V. Nebendahl, D. Nigg, M. Chwalla, M. Hennrich, and R. Blatt, "Experimental repetitive quantum error correction," *Science*, vol. 332, no. 6033, pp. 1059–1061, 2011.

[Sch+14] R. Schirhagl, K. Chang, M. Loretz, and C. L. Degen, "Nitrogen-vacancy centers in diamond: Nanoscale sensors for physics and biology," *Annual Review of Physical Chemistry*, vol. 65, pp. 83–105, 2014.

[Sch+16] E. Schoute, L. Mancinska, T. Islam, I. Kerenidis, and S. Wehner, "Shortcuts to quantum network routing," *arXiv preprint arXiv:1610.05238*, 2016.

[Sch+17] M. Schioppo, R. C. Brown, W. F. McGrew, N. Hinkley, R. J. Fasano, K. Beloy, T. Yoon, G. Milani, D. Nicolodi, J. Sherman, *et al.*, "Ultrastable optical clock with two cold-atom ensembles," *Nature Photonics*, vol. 11, no. 1, pp. 48–52, 2017.

[Sch01] D. Schlingemann, "Stabilizer codes can be realized as graph codes," *arXiv preprint quant-ph/0111080*, 2001.

[Sch05] M. Schlosshauer, "Decoherence, the measurement problem, and interpretations of quantum mechanics," *Reviews of Modern Physics*, vol. 76, no. 4, p. 1267, 2005.

[Sch17] R. Schnabel, "Squeezed states of light and their applications in laser interferometers," *Physics Reports*, vol. 684, pp. 1–51, 2017.

[Sch26] E. Schrödinger, "An undulatory theory of the mechanics of atoms and molecules," *Physical Review*, vol. 28, no. 6, p. 1049, 1926.

[Sch35] ——, "Die gegenwärtige situation in der quantenmechanik," *Naturwissenschaften*, vol. 23, no. 49, pp. 823–828, 1935.

[Sek+17] P. Sekatski, M. Skotiniotis, J. Kołodyński, and W. Dür, "Quantum metrology with full and fast quantum control," *Quantum*, vol. 1, p. 27, 2017.

[Sew+12] R. Sewell, M. Koschorreck, M. Napolitano, B. Dubost, N. Behbood, and M. Mitchell, "Magnetic sensitivity beyond the projection noise limit by spin squeezing," *Physical Review Letters*, vol. 109, no. 25, p. 253 605, 2012.

[Sha+18] R. Shaniv, T. Manovitz, Y. Shapira, N. Akerman, and R. Ozeri, "Toward heisenberg-limited rabi spectroscopy," *Physical Review Letters*, vol. 120, no. 24, p. 243 603, 2018.

[She+21] N. Shettell, W. J. Munro, D. Markham, and K. Nemoto, "Practical limits of error correction for quantum metrology," *New Journal of Physics*, vol. 23, no. 4, p. 043 038, 2021.

[She03] D. J. Sheskin, *Handbook of parametric and nonparametric statistical procedures*. Chapman and Hall/CRC, 2003.

[SHF13] K. M. Svore, M. B. Hastings, and M. Freedman, "Faster phase estimation," *arXiv preprint arXiv:1304.0741*, 2013.

[Sho94] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, Ieee, 1994, pp. 124–134.

[Sho95] ——, "Scheme for reducing decoherence in quantum computer memory," *Physical Review A*, vol. 52, no. 4, R2493, 1995.

[SJS17] D. S. Simon, G. Jaeger, and A. V. Sergienko, "Quantum metrology," in *Quantum Metrology, Imaging, and Communication*, Springer, 2017, pp. 91–112.

[SK20] J. S. Sidhu and P. Kok, "Geometric perspective on quantum parameter estimation," *AVS Quantum Science*, vol. 2, no. 1, p. 014 701, 2020.

[SM] N. Shettell and D. Markham, "Quantum metrology with delegated tasks," *in preparation*,

[SM05] M. Sarovar and G. J. Milburn, "Continuous quantum error correction by cooling," *Physical Review A*, vol. 72, no. 1, p. 012 306, 2005.

[SM20] N. Shettell and D. Markham, "Graph states as a resource for quantum metrology," *Physical Review Letters*, vol. 124, no. 11, p. 110 502, 2020.

[SMK21] N. Shettell, D. Markham, and E. Kashefi, "A cryptographic approach to quantum metrology," *arXiv preprint arXiv:2101.01762*, 2021.

[Son+17] C. Song, K. Xu, W. Liu, C.-p. Yang, S.-B. Zheng, H. Deng, Q. Xie, K. Huang, Q. Guo, L. Zhang, *et al.*, "10-qubit entanglement and parallel logic operations with a superconducting circuit," *Physical Review Letters*, vol. 119, no. 18, p. 180 511, 2017.

[SSD16] P. Sekatski, M. Skotiniotis, and W. Dür, "Dynamical decoupling leads to improved scaling in noisy quantum metrology," *New Journal of Physics*, vol. 18, no. 7, p. 073 034, 2016.

[Ste96a] A. M. Steane, "Error correcting codes in quantum theory," *Physical Review Letters*, vol. 77, no. 5, p. 793, 1996.

[Ste96b] ——, "Simple quantum error-correcting codes," *Physical Review A*, vol. 54, no. 6, p. 4741, 1996.

[Str+07] S. Strauf, N. G. Stoltz, M. T. Rakher, L. A. Coldren, P. M. Petroff, and D. Bouwmeester, "High-frequency single-photon source with polarization control," *Nature Photonics*, vol. 1, no. 12, pp. 704–708, 2007.

[Suz19] J. Suzuki, "Information geometrical characterization of quantum statistical models in quantum estimation theory," *Entropy*, vol. 21, no. 7, p. 703, 2019.

[SW01] D. Schlingemann and R. F. Werner, "Quantum error-correcting codes associated with graphs," *Physical Review A*, vol. 65, no. 1, p. 012 308, 2001.

[SW02] B. Schumacher and M. D. Westmoreland, "Approximate quantum error correction," *Quantum Information Processing*, vol. 1, no. 1, pp. 5–12, 2002.

[SW10] S. Schirmer and X. Wang, "Stabilizing open quantum systems by markovian reservoir engineering," *Physical Review A*, vol. 81, no. 6, p. 062 306, 2010.

[SZ03] H.-J. Sommers and K. Zyczkowski, "Bures volume of the set of mixed quantum states," *Journal of Physics A: Mathematical and General*, vol. 36, no. 39, p. 10 083, 2003.

[TA14] G. Tóth and I. Apellaniz, "Quantum metrology from a quantum information science perspective," *Journal of Physics A: Mathematical and Theoretical*, vol. 47, no. 42, p. 424 006, 2014.

[TAD20] M. Tsang, F. Albarelli, and A. Datta, "Quantum semiparametric estimation," *Physical Review X*, vol. 10, no. 3, p. 031 023, 2020.

[Tak+19a] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, "Resource-efficient verification of quantum computing using serfling's bound," *npj Quantum Information*, vol. 5, no. 1, pp. 1–8, 2019.

[Tak+19b] Y. Takeuchi, Y. Matsuzaki, K. Miyanishi, T. Sugiyama, and W. J. Munro, "Quantum remote sensing with asymmetric information gain," *Physical Review A*, vol. 99, no. 2, p. 022 325, 2019.

[Tam+14] T. H. Taminiau, J. Cramer, T. van der Sar, V. V. Dobrovitski, and R. Hanson, "Universal control and error correction in multi-qubit spin registers in diamond," *Nature Nanotechnology*, vol. 9, no. 3, pp. 171–176, 2014.

[Tay+08] J. Taylor, P. Cappellaro, L. Childress, L. Jiang, D. Budker, P. Hemmer, A. Yacoby, R. Walsworth, and M. Lukin, "High-sensitivity diamond magnetometer with nanoscale resolution," *Nature Physics*, vol. 4, no. 10, pp. 810–816, 2008.

[TB07] H. L. V. Trees and K. L. Bell, *Bayesian bounds for parameter estimation and nonlinear filtering/tracking*. Wiley-IEEE press New York, 2007.

[TB16] M. A. Taylor and W. P. Bowen, "Quantum metrology and its application in biology," *Physics Reports*, vol. 615, pp. 1–59, 2016.

[Til+10] T. Tilma, S. Hamaji, W. Munro, and K. Nemoto, "Entanglement is not a critical resource for quantum metrology," *Physical Review A*, vol. 81, no. 2, p. 022 108, 2010.

[TM18] Y. Takeuchi and T. Morimae, "Verification of many-qubit states," *Physical Review X*, vol. 8, no. 2, p. 021 060, 2018.

[TM20] G. Torlai and R. G. Melko, "Machine-learning quantum states in the nisq era," *Annual Review of Condensed Matter Physics*, vol. 11, pp. 325–344, 2020.

[Toy+13] D. M. Toyli, F. Charles, D. J. Christle, V. V. Dobrovitski, and D. D. Awschalom, "Fluorescence thermometry enhanced by the quantum coherence of single spins in diamond," *Proceedings of the National Academy of Sciences*, vol. 110, no. 21, pp. 8417–8421, 2013.

[Tsa13] M. Tsang, "Quantum metrology with open dynamical systems," *New Journal of Physics*, vol. 15, no. 7, p. 073 005, 2013.

[TWC11] M. Tsang, H. M. Wiseman, and C. M. Caves, "Fundamental quantum limit to waveform estimation," *Physical Review Letters*, vol. 106, no. 9, p. 090 401, 2011.

[UM20] A. Unnikrishnan and D. Markham, "Authenticated teleportation and verification in a noisy network," *Physical Review A*, vol. 102, no. 4, p. 042 401, 2020.

[Und+16] T. Unden, P. Balasubramanian, D. Louzon, Y. Vinkler, M. B. Plenio, M. Markham, D. Twitchen, A. Stacey, I. Lovchinsky, A. O. Sushkov, *et al.*, "Quantum metrology enhanced by repetitive quantum error correction," *Physical Review Letters*, vol. 116, no. 23, p. 230 502, 2016.

[Unn+19] A. Unnikrishnan, I. J. MacFarlane, R. Yi, E. Diamanti, D. Markham, and I. Kerenidis, "Anonymity for practical quantum networks," *Physical Review Letters*, vol. 122, no. 24, p. 240 501, 2019.

[Unr95] W. G. Unruh, "Maintaining coherence in quantum computers," *Physical Review A*, vol. 51, no. 2, p. 992, 1995.

[Van+06] M. Van den Nest, A. Miyake, W. Dür, and H. J. Briegel, "Universal resources for measurement-based quantum computation," *Physical Review Letters*, vol. 97, no. 15, p. 150 504, 2006.

[Van00] A. W. Van der Vaart, *Asymptotic statistics*. Cambridge university press, 2000, vol. 3.

[Van12] R. Van Meter, "Quantum networking and internetworking," *IEEE Network*, vol. 26, no. 4, pp. 59–64, 2012.

[Vid+14] M. D. Vidrighin, G. Donati, M. G. Genoni, X.-M. Jin, W. S. Kolthammer, M. Kim, A. Datta, M. Barbieri, and I. A. Walmsley, "Joint estimation of phase and phase diffusion for quantum metrology," *Nature Communications*, vol. 5, no. 1, pp. 1–7, 2014.

[Von18] J. Von Neumann, *Mathematical foundations of quantum mechanics: New edition*. Princeton university press, 2018.

[Wal+12] G. Waldherr, A. C. Dada, P. Neumann, F. Jelezko, E. Andersson, and J. Wrachtrup, "Distinguishing between nonorthogonal quantum states of a single nuclear spin," *Physical Review Letters*, vol. 109, no. 18, p. 180 501, 2012.

[Wal+14] G. Waldherr, Y. Wang, S. Zaiser, M. Jamali, T. Schulte-Herbrüggen, H. Abe, T. Ohshima, J. Isoya, J. Du, P. Neumann, *et al.*, "Quantum error correction in a solid-state hybrid spin register," *Nature*, vol. 506, no. 7487, pp. 204–207, 2014.

[Wan+17] Y. Wang, M. Um, J. Zhang, S. An, M. Lyu, J.-N. Zhang, L.-M. Duan, D. Yum, and K. Kim, "Single-qubit quantum memory exceeding ten-minute coherence time," *Nature Photonics*, vol. 11, no. 10, pp. 646–650, 2017.

[Wan+19] W. Wang, Y. Wu, Y. Ma, W. Cai, L. Hu, X. Mu, Y. Xu, Z.-J. Chen, H. Wang, Y. Song, *et al.*, "Heisenberg-limited single-mode quantum metrology in a superconducting circuit," *Nature Communications*, vol. 10, no. 1, pp. 1–6, 2019.

[Wan+21] W. Wang, Z.-J. Chen, X. Liu, W. Cai, Y. Ma, X. Mu, L. Hu, Y. Xu, H. Wang, Y. Song, *et al.*, "Quantum-enhanced radiometry via approximate quantum error correction," *arXiv preprint arXiv:2103.10281*, 2021.

[Was+10] W. Wasilewski, K. Jensen, H. Krauter, J. J. Renema, M. Balabas, and E. S. Polzik, "Quantum noise limited and entanglement-assisted magnetometry," *Physical Review Letters*, vol. 104, no. 13, p. 133 601, 2010.

[WCW14] T.-J. Wang, C. Cao, and C. Wang, "Linear-optical implementation of hyperdistillation from photon loss," *Physical Review A*, vol. 89, no. 5, p. 052 303, 2014.

[WEH18] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, 2018.

[Wei19] Z. Weinersmith. (2019). "Saturday morning breakast cereal: Quantum-2," [Online]. Available: https://www.smbc-comics.com/comic/quantum-2 (visited on 08/05/2021).

[Wen17] G. Wendin, "Quantum information processing with superconducting circuits: A review," *Reports on Progress in Physics*, vol. 80, no. 10, p. 106 001, 2017.

[Wes+01] D. B. West *et al.*, *Introduction to graph theory*. Prentice hall Upper Saddle River, 2001, vol. 2.

[WF20] Y. Wang and K. Fang, "Continuous-variable graph states for quantum metrology," *Physical Review A*, vol. 102, no. 5, p. 052 601, 2020.

[WG03] T.-C. Wei and P. M. Goldbart, "Geometric measure of entanglement and applications to bipartite and multipartite quantum states," *Physical Review A*, vol. 68, no. 4, p. 042 307, 2003.

[WG16] N. Wiebe and C. Granade, "Efficient bayesian phase estimation," *Physical Review Letters*, vol. 117, no. 1, p. 010 503, 2016.

[Wie83] S. Wiesner, "Conjugate coding," *ACM Sigact News*, vol. 15, no. 1, pp. 78–88, 1983.

[Wis+09] H. M. Wiseman, D. W. Berry, S. D. Bartlett, B. L. Higgins, and G. J. Pryde, "Adaptive measurements in the optical quantum information laboratory," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 15, no. 6, pp. 1661–1672, 2009.

[Woo81] W. K. Wootters, "Statistical distance and hilbert space," *Physical Review D*, vol. 23, no. 2, p. 357, 1981.

[WZ82] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[Xia+11] G.-Y. Xiang, B. L. Higgins, D. Berry, H. M. Wiseman, and G. Pryde, "Entanglement-enhanced measurement of a completely unknown optical phase," *Nature Photonics*, vol. 5, no. 1, pp. 43–47, 2011.

[Xie+18] D. Xie, C. Xu, J. Chen, and A. M. Wang, "High-dimensional cryptographic quantum parameter estimation," *Quantum Information Processing*, vol. 17, no. 5, p. 116, 2018.

[Xu+14] F. Xu, M. Curty, B. Qi, and H.-K. Lo, "Measurement-device-independent quantum cryptography," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 148–158, 2014.

[XWK87] M. Xiao, L.-A. Wu, and H. J. Kimble, "Precision measurement beyond the shot-noise limit," *Physical Review Letters*, vol. 59, no. 3, p. 278, 1987.

[Yin+13] M. Ying, N. Yu, Y. Feng, and R. Duan, "Verification of quantum programs," *Science of Computer Programming*, vol. 78, no. 9, pp. 1679–1700, 2013.

[Yin+20] P. Yin, Y. Takeuchi, W.-H. Zhang, Z.-Q. Yin, Y. Matsuzaki, X.-X. Peng, X.-Y. Xu, J.-S. Xu, J.-S. Tang, Z.-Q. Zhou, *et al.*, "Experimental demonstration of secure quantum remote sensing," *Physical Review Applied*, vol. 14, no. 1, p. 014 065, 2020.

[YL73] H. Yuen and M. Lax, "Multiple-parameter quantum estimation and measurement of nonselfadjoint observables," *IEEE Transactions on Information Theory*, vol. 19, no. 6, pp. 740–750, 1973.

[YMK86] B. Yurke, S. L. McCall, and J. R. Klauder, "Su (2) and su (1, 1) interferometers," *Physical Review A*, vol. 33, no. 6, p. 4033, 1986.

[Yok+13] S. Yokoyama, R. Ukai, S. C. Armstrong, C. Sornphiphatphong, T. Kaji, S. Suzuki, J.-i. Yoshikawa, H. Yonezawa, N. C. Menicucci, and A. Furusawa, "Ultra-large-scale continuous-variable cluster states multiplexed in the time domain," *Nature Photonics*, vol. 7, no. 12, pp. 982–986, 2013.

[ZAT00] K. Zetie, S. Adams, and R. Tocknell, "How does a mach-zehnder interferometer work?" *Physics Education*, vol. 35, no. 1, p. 46, 2000.

[ZC18] L. Zhang and K. W. C. Chan, "Scalable generation of multi-mode noon states for quantum multiple-phase estimation," *Scientific Reports*, vol. 8, no. 1, pp. 1–12, 2018.

[ZD14] Z. Zhang and L. Duan, "Quantum metrology with dicke squeezed states," *New Journal of Physics*, vol. 16, no. 10, p. 103 037, 2014.

[Zeh70] H. D. Zeh, "On the interpretation of measurement in quantum theory," *Foundations of Physics*, vol. 1, no. 1, pp. 69–76, 1970.

[ZH19a] H. Zhu and M. Hayashi, "Efficient verification of pure quantum states in the adversarial scenario," *Physical Review Letters*, vol. 123, no. 26, p. 260 504, 2019.

[ZH19b] ——, "General framework for verifying pure quantum states in the adversarial scenario," *Physical Review A*, vol. 100, no. 6, p. 062 335, 2019.

[Zha+13] Y. Zhang, X. Li, W. Yang, and G. Jin, "Quantum fisher information of entangled coherent states in the presence of photon loss," *Physical Review A*, vol. 88, no. 4, p. 043 832, 2013.

[Zhe+15] Q. Zheng, L. Ge, Y. Yao, and Q.-j. Zhi, "Enhancing parameter precision of optimal quantum estimation by direct quantum feedback," *Physical Review A*, vol. 91, no. 3, p. 033 805, 2015.

[Zho+18] S. Zhou, M. Zhang, J. Preskill, and L. Jiang, "Achieving the heisenberg limit in quantum metrology using quantum error correction," *Nature Communications*, vol. 9, no. 1, pp. 1–11, 2018.

[ZJ20] S. Zhou and L. Jiang, "Optimal approximate quantum error correction for quantum metrology," *Physical Review Research*, vol. 2, no. 1, p. 013 235, 2020.

[ZPJ20] Q. Zhuang, J. Preskill, and L. Jiang, "Distributed quantum sensing enhanced by continuous-variable error correction," *New Journal of Physics*, vol. 22, no. 2, p. 022 001, 2020.

[Zur06] W. H. Zurek, "Decoherence and the transition from quantum to classical—revisited," in *Quantum Decoherence*, Springer, 2006, pp. 1–31.

[ZYL14] Q. Zheng, Y. Yao, and Y. Li, "Optimal quantum channel estimation of two interacting qubits subject to decoherence," *The European Physical Journal D*, vol. 68, no. 6, pp. 1–7, 2014.

[ZYL16] ——, "Optimal quantum parameter estimation in a pulsed quantum optomechanical system," *Physical Review A*, vol. 93, no. 1, p. 013 848, 2016.

[ZZS18] Q. Zhuang, Z. Zhang, and J. H. Shapiro, "Distributed quantum sensing using continuous-variable multipartite entanglement," *Physical Review A*, vol. 97, no. 3, p. 032 329, 2018.