Quantum Communications Report for Ofcom

Hlér Kristjánsson, Robert Gardner and Giulio Chiribella

July 22, 2021

Contents

About the authors

Prof Giulio Chiribella is a world-leading expert on quantum information theory and foundations, with around 200 scientific publications and over 5000 citations. He is a full professor at the University of Hong Kong, and previously held the position of full professor at the University of Oxford, where he is now a visiting professor. His research interests include the generalisation of quantum communication to paradigms where the transmission lines themselves are combined in a quantum manner, thus exploring the ultimate limits of communication in a quantum setting. Prof Chiribella won the prestigious Hermann Weyl Prize in 2010, and has has held various fellowships, including being chosen as one of the 1000 Talents of China (2012) and being appointed a CIFAR-Azrieli Global Scholar (2016), a Croucher Senior Research Fellow (2018) and an RGC Senior Research Fellow (2020).

Hlér Kristjánsson is a 3rd-year doctoral student at the University of Oxford, under the supervision of Prof Giulio Chiribella and Prof Jonathan Barrett, and holds an MSci degree in physics from Imperial College London. His research focuses on studying the communication capabilities arising when transmission lines are combined in a quantum configuration and, together with Prof Giulio Chiribella, co-authored one of the first systematic studies of such generalised communication scenarios [Chiribella and Kristjánsson, 2019] as well as several follow-up works. Hlér won the first prize student poster award at the 19th Asian Quantum Information Science Conference (AQIS'19) in Seoul, South Korea (2019) and the best student talk award at the Q-Turn International Conference (2020), and was selected as an invited speaker at the 18th International Conference on Quantum Physics and Logic (QPL) in 2021.

Robert Gardner is a 2nd-year doctoral student at Imperial College London, supervised by Dr Steve Kolthammer, as part of the Controlled Quantum Dynamics Centre for Doctoral Training. His work is focused on the experimental generation of quantum light, with applications in a range of areas including random number generation and quantum communication. He has previously worked on an optical set-up for quantum neural networks and is currently collaborating with Prof Chiribella's group on the experimental implementation using single photons of the extension of quantum Shannon theory proposed in [Chiribella and Kristjánsson, 2019].

1 Introduction

The advances in communication technology over the last 50 years have led to a revolution in the way people communicate across the globe. These advances have been powered by technologies centred around the physics of electromagnetic waves and electronic signals. Yet, at the fundamental level, nature is governed by the laws of quantum physics, which give rise to new possibilities unattainable with control only over the phenomena of traditional classical physics. Quantum communication makes use of the laws of quantum physics to transmit information via quantum particles, such as single photons of light.

At present, there are large efforts around the world to build quantum communication networks. These are primarily motivated by the first near-term application of quantum communication, namely quantum key distribution (QKD). QKD enables the possibility of perfectly secret communication, which is guaranteed purely by the laws of physics, instead of relying on assumptions about the computational capabilities of the eavesdropper [Bennett and Brassard, 1984, Ekert, 1991], which are subject to constant change with ever-evolving technologies. More generally, quantum physics enables the transmission of a new type of information: the *private information*, which describes how many bits can be securely transmitted through any given communication channel such that it is physically impossible for an eavesdropper to obtain any of the information.

A longer-term motivation of building quantum networks is the construction of a **quantum internet**, securely connecting quantum processors around the world [Wehner et al., 2018]. The advent of quantum computing is expected to revolutionise the possibilities of solving hard or resource-intensive computational problems, with applications ranging from cybersecurity to financial modelling and drug discovery. Yet, just as in the case of conventional computers, many computational problems require the combined effort of multiple interconnected processors, for example in distributed systems. Quantum computers operate on yet another new type of information, this time fundamentally distinct from the classical information of bits: *quantum information*, measured in **qubits**. This means that connecting multiple quantum computers together requires a reliable quantum communication network capable of transmitting qubits with minimum error and maximum security. Quantum networks would enable the possibility of both **distributed quantum computing**, where small quantum computers can be linked up to achieve superior computational power, and **quantum cloud computing**, where small quantum devices send data to a large quantum computer that acts as a data processing facility. A quantum internet would also have applications in a variety of other areas, such as scientific measurements and ultra precise clock synchronisation and GPS.

In practice, quantum networks are typically realised by sending **single photons of light** through optical fibres or free space. Information (classical or quantum) is encoded in controllable parameters of the photons, for example in their polarisation. It is also possible to encode qubits into novel states of light instead of using single photons, for example coherent states (which correspond to classical light generated by a laser) and squeezed states (which are a quantum form of light). In order to probe the nature of light at the quantum level, the

sender and receiver require access to specialised generation and detection devices, respectively, allowing them to control the properties of individual photons. Detection and generation of quantum light is an ongoing area of research, often requiring specific engineering for the quantum regime such as cryogenic temperatures for generators and detectors. Furthermore, generation and detection devices both require a quantum processor in order to appropriately encode and decode their message onto/from the states of successive photons.

Once a quantum communication network is in place, it can also be used for many more tasks than those that initially motivated their construction. For example, a quantum communication line could also be used to transmit ordinary classical information. There are several indications that the use of quantum resources can **boost the capacity of sending classical bits** through transmission lines. *Superdense coding* enables a sender and receiver to boost the capacity of the communication channel between them by up to a factor of 2, provided they share *entangled quantum states* prior to communication [Bennett and Wiesner, 1992]. The use of classical states of light together with non-classical measurement techniques has been theoretically shown to achieve a higher capacity through various realistic quantum channel models with Gaussian noise compared to using only classical measurement techniques [Giovannetti et al., 2004, Shapiro et al., 2005], for example up to a factor of 4 higher capacity for a line-of-sight free-space channel. Finally, the use of multiple transmission lines simultaneously in a quantum superposition (see the following paragraph) has been shown to be able to increase the classical capacity of certain quantum channels. For example, when two discrete qubit white noise channels, each with zero capacity individually, are used in a quantum superposition, their combined capacity can be up to 0.31 bits per channel use [Abbott et al., 2020]. However, it is important to note that at present these results are primarily theoretical with some experimental proofs of principle, and only in the long term will it become clear to what extent, and in what scenarios, their benefit will outweigh the costs of the quantum resources (entangled states, squeezed states, non-classical measurement techniques, etc.) in practice.

The advancements of classical communication were described by the theory known as Shannon theory, after its founder, Claude Shannon [Shannon, 1948]. The novel possibilities discussed above are described by **quantum Shannon theory**, which generalises classical Shannon theory by allowing information to be encoded in the states of quantum particles [Wilde, 2013]. In practice, information is typically encoded in the internal states of particles, such as the polarisation of a single photon. However, quantum theory applies not only to the internal information-carrying states of particles, but also to the *propagation* of the particles in space and time. As the iconic double-slit experiment illustrates, quantum particles can propagate simultaneously through multiple alternative trajectories. This means that until the quantum mechanical nature of the propagation of information carriers is considered, there is a sense in which the transition from classical to quantum Shannon theory is incomplete. In a series of recent works, a second level of quantisation of Shannon theory has been formulated, where both the information and its propagation in space and time are treated quantum mechanically [Ebler et al., 2018, Gisin et al., 2005, Abbott et al., 2020, Chiribella and Kristjánsson, 2019]. This opens up the possibility of a single particle travelling simultaneously through multiple com-

munication channels, as well as even more exotic configurations, where the interference of the alternative configurations has been shown to enable the possibility of higher communication rates, for both classical and quantum information, through noisy channels.

In summary, the motivations of building quantum communication networks are:

1. unconditionally secure communication, e.g. QKD (current)
2. quantum internet, e.g. for distributed quantum computing (future)
3. higher communication rates when sending classical information (potentially, future)

As can be seem from point 2, one of the major motivations for quantum communication is in fact to enable the possibility of utilising **quantum computing** to its full potential. Conversely, quantum communication also relies on the possibility of (some form of) quantum computing: in order to communicate (either classical or quantum) information between two communicating parties, they must each have access to (at least a simple type of) quantum processor in order to encode and decode the information. Nevertheless, many of the advantages of quantum communication are expected to become useful well before fault-tolerant quantum computers are ready. This is because many of the advantages of quantum communication rely only on simple properties of quantum theory, such as entanglement and no-cloning, which can already be exploited with only a few qubits [Wehner et al., 2018]. However, in order to demonstrate a computational advantage, a quantum computer must have more qubits than efficiently simulable on a classical computer – a task of immense experimental difficulty.

An important point to keep in mind when considering the benefits of quantum technologies throughout this report is that they cannot always be directly compared to existing classical technologies as a benchmark. This is partly due to the fact that quantum technologies have not yet reached the maturity of existing classical technologies, however, in many cases it is predominantly due to the fact that quantum provides radically new types of technologies, whose applications do not exist classically. For example, consider a network of distributed quantum computers connected using a quantum network. Quantum computers, which can perform tasks impossible on a conventional computer, all work with qubits, so it does not make sense to take traditional communication networks which work with bits as a reference point. This is perhaps analogous to the step from radio to television or from landline to mobile telecommunications.

In chapter 3, the various new possible communication scenarios of quantum Shannon theory are presented, together with their quantifications, namely, the transmission of classical information, private information, and quantum information. This is followed by several examples of quantum channels and their classical and quantum capacities, including a discussion of some potential advantages of using quantum methods to transmit classical information. Then, the notion of quantum networks and their current limitations are explored, and the chapter concludes with the recent extensions to a second level of quantisation of Shannon theory. Chapter 4 presents the experimental challenges in implementing the protocols of quantum communication in practice, followed by examples of current applications in chapter

5. The report concludes with a few short chapters outlining the timeline of advances, the major players in the field, and current industry standards. But first, in chapter 2, the report begins with a technical overview of the framework of quantum physics, outlining the basic mathematical tools needed to understand the discussions in the following chapters. In the following, familiarity with basic linear algebra, as taught in an undergraduate science or engineering degree, will be assumed.

2 Overview of Working Principles

In this section key features of classical and quantum information are outlined in order to enable a working understanding for the rest of the report. The shift from the classical to the quantum regime is described, including notions of state purity, evolution and measurements, quantum channels as well as composite systems and quantum entanglement. This section is technical, drawing inspiration from various sources [Nielsen and Chuang, 2000, Jennings, 2019, Chiribella, 2020] , but it is shortened to give essential information while still giving a deeper insight into the physics outlined later on in the report.

2.1 Classical and quantum information

Quantum theory acts as a paradigm shift compared to classical systems. This section introduces both classical and quantum theory via an 'operational approach', which explains classical and quantum state spaces in terms of simple, abstract systems in which probabilities and measurement play a central role. This view allows for a simple generalisation from classical to quantum systems and intuitively demonstrates why quantum states yield more logical freedom than their classical counterparts.

2.1.1 Classical systems

Classical systems and their measurements can be described vectorially. As an example, consider a coin, either in the 'heads' state or the 'tails' state. The degree of knowledge about the system is described by a probability distribution encoded in a state vector,

$$\mathbf{c} = (c_0, c_1)^t = \begin{pmatrix} \mathrm{P}(\mathrm{heads}) \\ \mathrm{P}(\mathrm{tails}) \end{pmatrix} \tag{1}$$

where P(x) is the probability of outcome x, and $(\cdots)^t$ is the transpose of a row vector. Complete uncertainty about the coin's state is represented by $\mathbf{c} = (\frac{1}{2}, \frac{1}{2})^t$ – which is known as the maximally mixed state – while certainty of, for example the 'heads' state, is described by $\mathbf{c} = (1, 0)^t$, which is known as a pure state of the system. Mixed states are therefore defined as mixtures of pure states. Evolutions of classical systems are ones in which a classical state is linearly transformed into another valid classical state. In a physical setting, evolutions describe any process through which a system develops, for instance, a pulse of light dispersing over time, or travelling through a length of fibre.

Measurements of classical systems can also be described through a set of r (row) vectors. The example of the coin above, with $r = 2$, is described via $\{\mathbf{m}_0, \mathbf{m}_1\}$ which can yield 2 potential different outcomes (although this can easily be generalised to higher-dimensional systems). Again, these can be defined by considering the outcome likelihoods; the probability

of measuring state **j** (i.e. the j$^{\text{th}}$ outcome from the measurement set) is given by,

$$\text{prob}(\mathbf{j}) = \mathbf{m}_j\mathbf{c} \tag{2}$$

where $\mathbf{m}_j$ is the j^{th} measurement vector. Following on from the previous example, a question such as *'is the system in the 'heads' state?'* is described by $\mathbf{m}_0 = (1, 0)$, with the alternative outcome being the 'tails' state, described through $\mathbf{m}_1 = (0, 1)$. Certain constraints apply: the components of each measurement vector must be non–negative and the sum of the probabilities for all possible outcomes must be 1,

$$\sum_{j=0}^{1} \text{prob}(\mathbf{j}) = \sum_{j=0}^{1} \mathbf{m}_j\mathbf{c} = 1 \rightarrow \sum_{j=0}^{1} \mathbf{m}_j = (1, 1). \tag{3}$$

Although there are a set of r measurement matrices, which give information on the probability of a particular outcome, in practice a measurement will yield only a single result $\mathbf{m}_j$. The matrix corresponding to the outcome of a measurement can then be used to consider how a system evolves after a measurement.

These ideas can be generalised to quantum systems, where a measurement of a coin could instead be generalised to the detection of a single photon; this yields some information on the photon's 'quantum state', as will be explored in the next section.

2.1.2 Quantum systems

Quantum systems have a larger state space than classical ones due to coherences between the pure states of the system; quantum states require matrices to describe them, instead of a vectorial representation.

As an example, the classical coin example can be embedded in quantum theory. With the correct basis choice, such that the eigenvectors of the matrix are valid classical pure state vectors, this can be represented as a diagonal matrix,

$$\rho_{\text{classical}} = \begin{pmatrix} \text{P(heads)} & 0 \\ 0 & \text{P(tails)} \end{pmatrix}, \tag{4}$$

or, for more general two dimensional classical systems,

$$\rho_{\text{classical}} = \begin{pmatrix} c_0 & 0 \\ 0 & c_1 \end{pmatrix}, \tag{5}$$

where ρ is known as the *density matrix*, and, in the case of diagonal classical matrices, the components give the probability of different outcomes. The idea that classical theory is a subset of quantum theory is explored geometrically in section 2.1.3.

Moving to a generically quantum system, which will be expanded upon in later sections, consider a photon (a quanta, or particle, of light) which can travel from one system to another via two different routes. The classical pure states describe the cases in which the photon

definitely travels through one of the routes, for example route 0, represented through vector: $(1,0)^t$ and route 1, represented through the vector $(0,1)^t$. Different example classical situations are encoded via:

$$\rho_{\text{route}_0} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \rho_{\text{route}_1} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \rho_{\text{unknown}} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \tag{6}$$

where ρ_{unknown} is the classical state where we have no information about which route the photon travelled, i.e. where a flat prior (equal uncertainty about each path) is applied to the system. States beyond the classical theory have non–zero off diagonal elements (in this classical basis choice), known as coherences. These describe quantum states that are in a superpositon of various classical states – this is the case where the photon travels down both route 0 and route 1 simultaneously. This will be explored more fully in section 2.3.

For completeness, this section can be considered technically. To move from classical to quantum theory, vectors are replaced by Hermitian matrices, the non-negativity of vector components is instead applied to the eigenvalues of the matrices, and traces are used instead of vector products.

To clarify, Hermitian matrices are the complex generalisation of symmetric matrices (where matrix $\hat{S} = \hat{S}^t$) i.e. a matrix is its own transpose. In the complex case, $t \rightarrow \dagger$ where $\dagger$ is a transpose followed by complex conjugation of all the matrices elements. If matrix $\hat{H}$ is Hermitian, this means that $\hat{H} = \hat{H}^\dagger$.

Using these replacement rules, classical state vectors **c** become Hermitian matrices ρ known as density matrices (as shown in the example above), while measurement vectors become a set of Hermitian matrices M_j. Probability conservation is held in a new condition: $\text{Tr}(\rho) = 1$, which is the trace of the density matrix, given by the sum of its diagonal components. For measurements, the condition $\sum_{j=0}^{1} \mathbf{m}_j = (1,1)$ becomes $\sum_{j=0}^{1} M_j = I_2$, where I_2 is the 2-dimensional identity matrix.

The probability of an outcome ρ_j (i.e. the state described by the j^{th} outcome of the measurement set) is given by,

$$\text{prob}(\rho_j) = \text{Tr}(M_j \rho) \tag{7}$$

Evolutions of quantum states (for example the change in a photon's state when travelling through a noisy communication channel), which will be described more fully in section 2.3, are linear transformations from $\rho \rightarrow \mathcal{E}(\rho)$, where both ρ and $\mathcal{E}(\rho)$ are valid density matrices.

2.1.3 Qubits and the Bloch Ball

Qubits are the quantum counterparts of classical bits – described by (2×2) Hermitian matrices; the travelling photon example above can be written in this form. It is known that any valid (2×2) density matrix can be uniquely decomposed into a sum of so-called Pauli matrices,

$$\rho = \frac{1}{2}(\hat{I} + x\hat{X} + y\hat{Y} + z\hat{Z}) \tag{8}$$

$$\hat{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \hat{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \hat{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \hat{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{9}$$

with $x^2 + y^2 + z^2 \leq 1$ required for positive eigenvalues. Any unique qubit state can therefore be described by these three components (x, y, z). Geometrically, a so-called Bloch vector can be constructed as,

$$\mathbf{r} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}, |\mathbf{r}| \leq 1 \tag{10}$$

with all possible qubit states mapping out the space of a sphere, known as the Bloch Ball, shown in figure 1. Classical states have diagonal density matrices, which means their (x,y) components are zero; geometrically this confines all classical states to the the z-axis, with opposing ends representing the two possible classical pure states (i.e. $z = \pm 1$) and the center being the maximally mixed state ($z = 0$).

Considering a classical optical system, the Bloch Ball corresponds directly to the Poincaré Sphere in the case of a photon's polarisation. In this instance, the 'classical' pure states on the z-axis are the vertical and horizontal polarisation states, the x-axis describes linear mixtures of these, yielding diagonal and anti–diagonal polarisations, while the y-axis, which introduces an imaginary component, gives rise to circularly polarised states. Elliptically polarised states lie elsewhere on the surface of the sphere.

The Bloch Ball however also encompasses qubits more generally, for example as mentioned above, a photon's spatial state, corresponding to travelling through one of two separate paths, can be considered as a qubit. The classical pure states (on the z-axis) represent the photon definitively travelling down a particular path, while more general states, with the photon travelling down a superposition of both paths lie on different parts of the Bloch Ball.

2.1.4 Dirac notation

Dirac notation greatly simplifies quantum theory and its presentation. For qubits, states are typically mapped onto 'kets' in the following way:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{11}$$

while their Hermitian conjugates (transpose with complex conjugation) are mapped onto 'bras',

$$\langle 0| = \begin{pmatrix} 1, & 0 \end{pmatrix}, \langle 1| = \begin{pmatrix} 0, & 1 \end{pmatrix} \tag{12}$$

which means that $|n\rangle^\dagger = \langle n|$. Inner products are therefore succinctly represented through,

$$\begin{pmatrix} \alpha_0^*, & \alpha_1^* \end{pmatrix} \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \sum_{i=0}^{1} \alpha_i^* \beta_i = \langle \alpha | \beta \rangle . \tag{13}$$

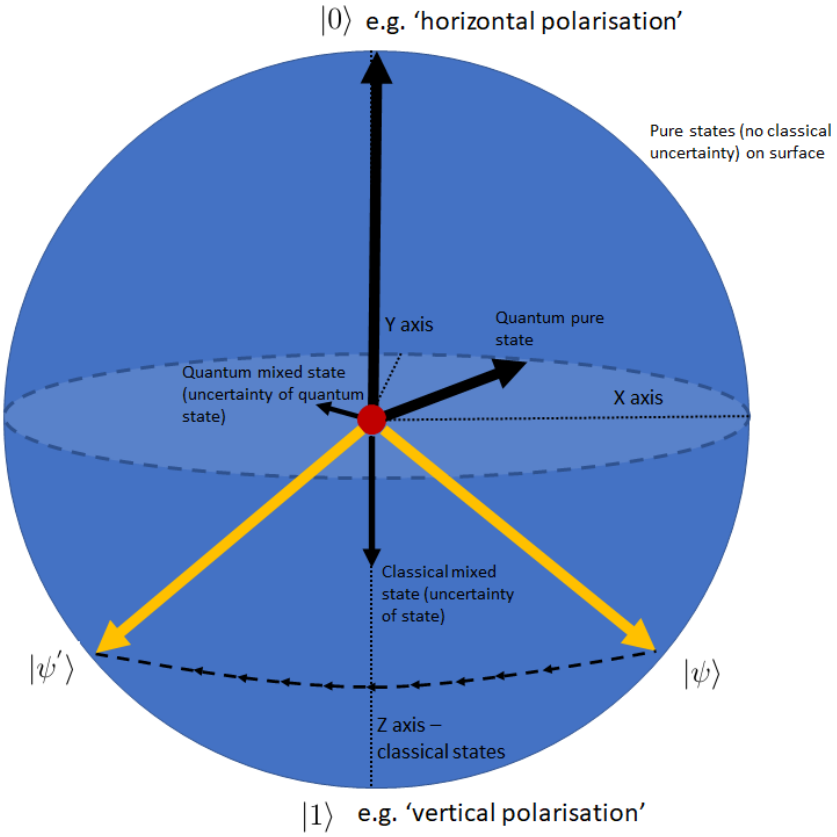

Figure 1: The Bloch Ball. Bloch vectors have a length proportional to their width. The center is the maximally mixed state (red), while all classical states lie on the Z axis. Pure states lie on the ball's surface, and single qubit unitary evolutions are represented as rotations of the Bloch vector (e.g. the trajectory in yellow).

In general, basis vectors are chosen to be orthonormal, with $\langle m|n\rangle = \delta_{mn}$. Matrices can be formed via an outer product, for example,

$$|\beta\rangle\langle\alpha| = \begin{pmatrix} \beta_0\alpha_0^* & \beta_0\alpha_1^* \\ \beta_1\alpha_0^* & \beta_1\alpha_1^* \end{pmatrix} \tag{14}$$

which is a matrix of dimension 2×2.

When considering the previous example of a travelling photon, density matrices can instead be represented as $\rho_{\text{route}_0} = |0\rangle\langle 0|$, $\rho_{\text{route}_1} = |1\rangle\langle 1|$ (pure states) and $\rho_{\text{unknown}} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$ (the maximally mixed state).

Matrices, which act as operators in quantum theory, can also be applied directly to bras and kets (vectors). Applying a matrix $\hat{A}$ to $|n\rangle$ (represented as a vector) is written $\hat{A}|n\rangle$, and the Hermitian conjugate of this object is given by $(\hat{A}|n\rangle)^\dagger = \langle n|\hat{A}^\dagger$; this is especially useful for interpreting properties of quantum states. These matrices can also be placed between inner products – for instance $\langle m|\hat{A}|n\rangle$ – yielding a (complex) number.

2.2 Further aspects of quantum theory

Armed with a knowledge of Dirac notation, and the idea that quantum theory is more general than classical theory, further ideas can be introduced. In particular this section goes into more detail about quantum states as well as their evolution and measurement.

2.2.1 Pure and mixed states

The Dirac notation formalism gives an easy route to introducing the idea of pure and mixed states in the quantum regime (these have already been defined for a classical system). The geometric interpretation from the Bloch Ball is useful here. Pure states exist on the surface of the Bloch Ball, with a Bloch vector $|\mathbf{r}| = 1$, while mixed states are ones inside the sphere $|\mathbf{r}| < 1$.

It is known that for quantum pure states, their density matrix can be decomposed into the outer–product of a so–called state–vector with itself, while quantum mixed states can only be described by a (weighted) sum of pure states,

$$\rho_{\text{pure}} = |\psi\rangle\langle\psi| \tag{15}$$

$$\rho_{\text{mixed}} = \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{16}$$

with the probabilities p_i satisfying $\sum_i p_i = 1$, as required for normalisation. This has an intuitive interpretation – quantum mixed states are ones where there is a classical uncertainty of the quantum state of the system; this is analogous to the classical situation. For example, consider a system with two quantum pure states ρ_0 and ρ_1, with complete uncertainty about which state the system is in. The system is therefore described through a mixed state $\rho_{\text{mixed}} =$

$\frac{1}{2}(\rho_0 + \rho_1)$. It is clear that in the example of the travelling photon, $\rho_{\text{route}_0} = |0\rangle\langle 0|$ and $\rho_{\text{route}_1} = |1\rangle\langle 1|$ are both pure states, while $\rho_{\text{unknown}} = \frac{1}{2}(\rho_{\text{route}_0} + \rho_{\text{route}_1})$ is a mixed state.

Turning to pure states – which are represented by the outer product of a state vector with itself – any state vector of a quantum state is given by a superposition of basis vectors (which are typically chosen to represent classical pure states),

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{17}$$

with $|\alpha|^2 + |\beta|^2 = 1$. For pure states, because all the information about the system is encoded in the state–vector (i.e. the full density matrix is partly redundant), it is often the case that the dynamics of a system are computed with $|\psi\rangle$ rather than $\rho = |\psi\rangle\langle\psi|$.

Although less general, pure states are often easier to interpret. Classical pure states consist of a single basis vector (e.g. $|\psi\rangle = |0\rangle \rightarrow \rho_{\text{route}_0} = |0\rangle\langle 0|$), while truly quantum states, which, for qubits, are not on the z-axis of the Bloch Ball, consist of multiple basis vectors – and describe superpositions of classical states. For example,

$$|\psi\rangle_{\text{superposition}} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{18}$$

$$\rho_{\text{superposition}} = |\psi\rangle\langle\psi| = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \tag{19}$$

which clearly has off-diagonal components and cannot be described by a classical theory. Importantly, this is distinct from a mixed classical state (e.g. ρ_{unknown} in the travelling photon example) which has no coherences between its classical pure states (i.e. no off-diagonal elements in its density matrix).

2.2.2 Superposition and coherence

The idea of superposition and coherence is central to quantum theory and can be placed on firmer footing. A key example is the double slit experiment, shown in figure 2. In this experiment, a photon is sent through two slits and hits a detection plane on the other side. The classical pure states are represented as the photon travelling through the left slit $\rho_{\text{route}_0} = |0\rangle\langle 0|$ or else, travelling through the right slit $\rho_{\text{route}_1} = |1\rangle\langle 1|$. Sending many photons will build up a pattern on the detection plane, and this depends on whether the photon hitting the plane is in a classical or quantum state.

If the photons that hit the plane are in either ρ_{route_0} or ρ_{route_1} (or a classical mixture of these), the detection screen will consist of two bright bands, where the photon has definitively travelled through one of the two slits. However if the photon is in the state $\rho_{\text{superposition}} = |\psi\rangle\langle\psi|$, with $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, then the photon, in some sense, travels simultaneously through both slits and will give rise to an interference pattern on the plane, consisting of many bands; this can be thought of as arising because of the off–diagonal coherences in the photon's

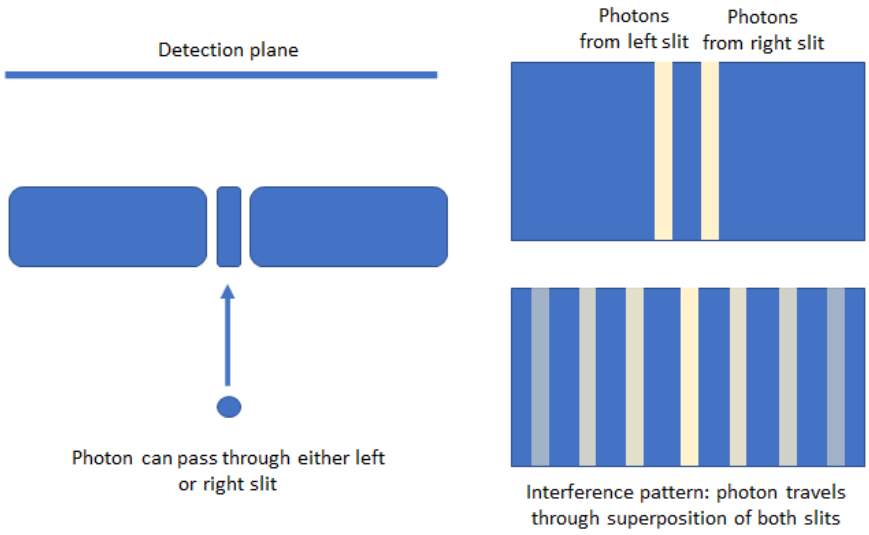

Figure 2: The double slit experiment. Classical states give rise to the two band pattern on the detection plane, while superposition states create an interference pattern.

density matrix.

It is also possible to create conditions which will decay the coherences and cause the classical detection pattern to arise. *Decoherence* is the term used for any process where the coherences, the off-diagonal terms, are reduced, ultimately resulting in a classical state. For this example,

$$\rho_{\text{superposition}} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \rightarrow \rho_{\text{classical}} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{20}$$

which shows the off–diagonal components are no longer present. Of importance is the notion of *coherence time*, which is the timescale on which a quantum state remains coherent – decoherence happens naturally, and is a key obstacle in maintaining quantum information in quantum systems. Moreover, for photons to interfere with one another and, in general to perform joint quantum operations, they should be close to indistinguishable. This means they share the same properties, including frequency, spatial mode and polarisation, and this is explored more thoroughly in section 4.2.

2.2.3 Reversible evolution

Quantum states change over time, subject to interactions, for example when a state is sent through a noisy communication channel. To be a valid evolution, one quantum density matrix must be mapped to another valid density matrix (or state–vector for pure states). If an evolution did not have this constraint, quantum theory would give rise to unphysical situations e.g. ones which do not conserve probability. The updated density matrix must have $\text{Tr}(\rho) = 1$ and positive eigenvalues. These evolutions are, in general, described by completely positive, trace-preserving (CPTP) maps. Reversible evolutions are a subset of these maps, in which the

evolution from an one state to another is possible in both directions. This is to say that, there exist evolutions outside this regime which will take quantum state ρ to quantum state ρ', but that it is impossible to return from ρ' to ρ; an example includes loss in optical systems.

Reversible evolutions are described with unitary matrices. In analogy to how Hermitian matrices are the complex generalisation of symmetric matrices, unitary matrices are the complex generalisation of orthogonal matrices . Orthogonal matrices obey $\hat{O}^t = \hat{O}^{-1}$ where $\hat{O}^{-1}$ is the matrices inverse, while unitary matrices therefore obey $\hat{U}^\dagger = \hat{U}^{-1}$. Considering pure states, these operators can be applied directly to state vectors to evolve a quantum state

$$|\psi'\rangle = \hat{U}\,|\psi\rangle\,, \tag{21}$$

$$\hat{U}^{-1}\,|\psi'\rangle = |\psi\rangle\,, \tag{22}$$

where $\hat{U}$ is a unitary matrix obeying the relation $\hat{U}^\dagger = \hat{U}^{-1}$. (In this chapter, matrices acting on quantum states in this way are denoted with a hat for emphasis; this notation will be suppressed in later chapters.) By considering the fact that for mixed states, $\rho = \sum_i p_i\,|\psi_i\rangle\,\langle\psi_i|$, it can be seen that reversible evolutions for general quantum states act as,

$$\rho^{'} = \hat{U}\rho\hat{U}^\dagger, \tag{23}$$

where ρ' is another valid density matrix. Such evolutions are useful, for instance, in describing closed systems, such as a photon travelling through a lossless beam–splitter. Reversible operations are not the most general form of quantum evolution however; they do not include open systems, environmental interactions or projective measurements which are also key elements of quantum theory – these evolutions are more generally described via quantum channels, which are outlined in section 2.2.5.

As a concrete example for a pure state qubit, a unitary evolution will take $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \rightarrow |\psi'\rangle = \alpha^{'}\,|0\rangle + \beta^{'}\,|1\rangle$, which is a different qubit pure state. Unitary evolutions allow complete control over the values of $\alpha^{'}$ and $\beta^{'}$, and geometrically will rotate a qubit's Bloch vector around the Bloch Ball. This is important for performing single-qubit gate operations, which are necessary for processing the received qubits in communication.

2.2.4 Measurements

Measurements have an important role in quantum theory, and can be introduced by considering the travelling photon example from previous sections. A measurement of the photon would require single photon detectors on both route 0 and route 1. In this instance, a measurement is analogous to photon detection; a click on the detector gives information about the photon's quantum state. Now, consider the case where the photon is in a quantum superposition state, $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, travelling down both routes 'simultaneously'. When a measurement occurs, one of the detectors clicks, registering the photon; this is a genuinely random process governed by quantum theory. The probability of the photon being detected in route 0 is $|\alpha|^2$, while the probability of being detected in route 1 in $|\beta|^2$. Since $|\alpha|^2 + |\beta|^2 = 1$, probability is

conserved, and the photon will definitely be detected in one of the arms (there is no loss in this system).

In this case, the photon is destroyed upon measurement, due to the physical nature of single photon detectors. In general however, a measurement will evolve the quantum state in a non-trivial way, 'collapsing' it to a classical state. In the travelling photon example, a measurement of the photon on route 0 would hypothetically evolve the photon's state $|\psi\rangle \rightarrow |0\rangle$, while a measurement on route 1 would cause the evolution $|\psi\rangle \rightarrow |1\rangle$. This evolution is not reversible and cannot be described by a unitary matrix.

Again measurements can be placed on firmer footing, using the theory outlined in section 2.1.2. where it was seen that a measurement can be described by a set of matrices $\{M_0, M_1, \ldots, M_{r-1}\}$, with r distinct potential outcomes, $\sum_{j=0}^{r-1} M_j = \hat{I}$ and the probability of the j^{th} outcome, $\text{prob}(\rho_j) = \text{Tr}(M_j \rho)$. In this setting, each measurement matrix is orthogonal to each other and described by 'projectors'. In the qubit regime, an example measurement set would be $\{M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|\}$, an example being a question of the form *'is the travelling photon on route 0 or route 1?* As mentioned above, quantum states update after measurements. A subtlety is involved here – the outputted state is generally not normalised (the trace of the updated state's density matrix is not one), and so this needs to be renormalised manually – known as the measurement update.

2.2.5 Quantum channels

Evolutions of quantum states are not limited by reversible processes and measurements – irreversible processes are also possible, and a unifying framework to describe any evolution can be introduced by considering quantum channels.

As a simple example, consider a photon which has its quantum state encoded in its polarisation (rather than spatial position as in the travelling photon example). In this case, a photon with horizontal polarisation is given by $|H\rangle = |0\rangle$, while vertical polarisation is described by $|V\rangle = |1\rangle$, which represent the two end points of the z-axis on the Bloch Ball.

Unitary evolution and measurements are not general enough to describe probabilistic errors. This instead requires the notion of a *quantum channel*. Consider a bit-flip error $|H\rangle \leftrightarrow |V\rangle$ which happens to the photon with probability p (e.g. the case where the photon's polarisation state is rotated by a phase of $\frac{\pi}{2}$). Mathematically, the quantum bit-flip channel acting on any input quantum state ρ (i.e. any polarisation input state) is given by

$$\mathcal{E}_{\text{bit-flip}}(\rho) = (1-p)\rho + pX\rho X, \tag{24}$$

where X is the Pauli X matrix (see eq. (8)) which swaps $|0\rangle = |H\rangle$ and $|1\rangle = |V\rangle$. This is an example of a quantum channel, which, in general, are described by,

$$\mathcal{E}(\rho) = \sum_{i=0}^{n-1} \hat{K}_i \rho \hat{K}_i^\dagger, \tag{25}$$

where $\mathcal{E}(\rho)$ is the input quantum density matrix after evolution (i.e. an alternative notation to ρ'), and the set $\{\hat{K}_i\}$ are known as Kraus operators. In the example above, two Kraus operators are involved, $\hat{K}_0 = \sqrt{1-p}I, \hat{K}_1 = \sqrt{p}X$. This formalism allows for a description of any physical quantum evolution.

The form of quantum channels comes from the fact that all quantum channels are described by completely positive, trace-preserving (CPTP) maps. Fitting this with the framework developed earlier in the chapter, the evolution is totally described by a set of n Kraus operators $\{\hat{K}_0, \hat{K}_1, \ldots, \hat{K}_{n-1}\}$ which are represented through matrices; these satisfy the condition that $\sum_{i=0}^{n-1} \hat{K}_i^\dagger \hat{K}_i = \hat{I}_n$. . Reversible dynamics and measurements are a subset of the evolutions described by quantum channels. This can be seen explicitly by considering the case for $n = 1$, in which the evolution reduces to unitary (reversible) dynamics $\hat{K}_0 = \hat{U}$, since $\sum_{i=0} \hat{K}_0^\dagger \hat{K}_0 = \hat{U}^\dagger \hat{U} = \hat{I}$. For $n \geq 2$ the system is evolving in a way analogous to measurements, but with no renormalisation – answers to the set of measurement questions such as 'is the system in state $|0\rangle$?' are being updated, although a measurement is not explicitly performed and no measurement update is required.

2.2.6 How many bits fit in a qubit and how many qubits fit in a photon

Given a quantum system which involves,

1. state preparation, e.g. of $|0\rangle$, $|1\rangle$ or some superposition state
2. state evolution through a quantum channel
3. state measurement, which causes the quantum state to collapse to a classical one,

and the fact that classical states are a subset of quantum ones (i.e. the z–axis of the Bloch Ball), it could be asked whether or not quantum states can store or transmit more classical information than classical systems of the same dimension.

This question is addressed by the Holevo bound [Holevo, 1973]. Although a set of n qubits can represent a large amount of classical information (2^n complex numbers), measurement collapse limits the amount of decodable information to n classical bits. This gives an upper bound to the number of bits that can be stored in a qubit: a single qubit can only store and transmit a single bit of classical information. Note that this is separate from the question of how many bits/qubits can be transmitted through a given communication channel – this is quantified by the capacity of a noisy channel, discussed in §3.

However, note that this bound applies to the encoding of quantum states without additional resources. With additional quantum resources such as shared entangled states between a sender and receiver, this bound can be exceeded using protocols such as superdense coding (see section 5).

At this point, it is important to stress the distinction between a single *qubit* and a single *particle* (e.g. photon). A photon is a particle of light (see §4 for more detail), and in many communication scenarios, a single photon is used as a single qubit, e.g. by assigning its opposite

polarisation states to the $|0\rangle$ and $|1\rangle$ qubit basis states. However, in general, a single qubit could correspond to a joint state of multiple photons, or alternatively, a single photon could correspond to multiple qubits, depending entirely on the way in which the qubit is encoded in the physical variables of the photon(s).

For example, as we have seen above from the double slit experiment, the path a photon takes can also be associated with a qubit – the left-hand path corresponds to $|0\rangle$ and the right-hand path corresponds to $|1\rangle$. Now, if both the polarisation and the path variables (or 'degrees of freedom') of the photon are used as qubits, then the photon corresponds to 2 qubits. In addition to polarisation and path, a single photon has many other degrees of freedom which can be used to encode information, such as angular momentum and time-bins, which are discussed later in the report in §3.1. Alternatively, a qubit can be encoded in the number of photons present: $|0\rangle$ corresponds to no photons, $|1\rangle$ to a single photon. It is even possible to encode qubits in continuous variable systems – see §2.4 – where the $|0\rangle$ and $|1\rangle$ qubit basis states correspond to different superpositions of multiple photon-number states, of the form $\alpha_0 \,|0 \,\text{photons}\rangle + \alpha_1 \,|1 \,\text{photon}\rangle + \alpha_2 \,|2 \,\text{photons}\rangle + \ldots$, where the α_i are complex numbers.

This means that the Holevo bound only applies to the information-theoretic concept of qubit, but does not say anything about the number of bits that fit in any particular quantum particle. The number of bits or qubits that can be encoded in a single photon is really an engineering question, which depends on the technologies available for generating and detecting the different degrees of freedom of a photon – discussed in §4. For current practical purposes, the most common scenario is using only the polarisation of a photon to carry information, in which case a single photon just corresponds to a single qubit. However, research is underway to determine the most resource-efficient encodings involving multiple degrees of freedom [Piparo et al., 2020].

2.3 Multiple quantum systems

At present only single systems have been considered. A central feature of quantum mechanics is entanglement between multiple different systems, which has important applications in quantum information and communication. The analysis in this section is restricted to pure states – dynamics are computed using $|\psi\rangle$ rather than ρ. This simplifies explanations without taking away any core ideas.

Ideas in this section are introduced intuitively; for a fuller, technical account of composite systems and entanglement, see Appendix A.

2.3.1 Introducing the tensor product

Consider two quantum states in separate systems, $|\psi_a\rangle$ in system 'a' and $|\psi_b\rangle$ in system 'b',

$$|\psi_a\rangle = \alpha_a \,|0\rangle + \beta_a \,|1\rangle = \begin{pmatrix} \alpha_a \\ \beta_a \end{pmatrix} \tag{26}$$

$$|\psi_b\rangle = \alpha_b |0\rangle + \beta_b |1\rangle = \begin{pmatrix} \alpha_b \\ \beta_b \end{pmatrix}$$

Then the state in the combined total system – system 'c' – can be constructed via a tensor product of each state vector,

$$|\psi_c\rangle = |\psi_a\rangle \otimes |\psi_b\rangle = \begin{pmatrix} \alpha_a\alpha_b \\ \alpha_a\beta_b \\ \beta_a\alpha_b \\ \beta_a\beta_b \end{pmatrix} \tag{27}$$

and an important shorthand used later is $|nm\rangle = |n\rangle \otimes |m\rangle$.

Objects act on states in an intuitive way in this picture as well – this includes kets, bras and matrices. For concreteness, consider matrix $\hat{A}$ which acts on $|\psi_a\rangle$ in system 'a' and matrix $\hat{B}$ which acts on $|\psi_b\rangle$ in system 'b'. It is possible to construct a matrix $\hat{C} = \hat{A} \otimes \hat{B}$ which acts appropriately on the combined 'c' system,

$$|\psi_a^{'}\rangle = \hat{A} |\psi_a\rangle \tag{28}$$

$$|\psi_b^{'}\rangle = \hat{B} |\psi_b\rangle$$

$$|\psi_c^{'}\rangle = \hat{C} |\psi_c\rangle = (\hat{A} \otimes \hat{B})(|\psi_a\rangle \otimes |\psi_b\rangle) = \hat{A} |\psi_a\rangle \otimes \hat{B} |\psi_b\rangle$$

which is a way of noting that each matrix acts independently from one another in subsystems 'a' and 'b'.

2.3.2 Product and entangled states

States that can be written in the form of

$$|\psi_N\rangle = |\psi_0\rangle \otimes |\psi_1\rangle \otimes ... \otimes |\psi_{n-1}\rangle \,, \tag{29}$$

are known as *product states*, and these do not contain any entanglement. Measuring one subsystem will be completely independent from all other subsystems, and there are no correlations across the different measurement results.

However, this is only a small subset of the possible set of composite quantum states. Most states cannot be written in this form – instead, they can only be written as a linear sum of product states, analogous to the way in which superposition states can only be written as a linear sum of classical pure states. Quantum states such as these are known as *entangled states*. As a concrete example, for a composite system of 2 subsystems, an example of an entangled state is the Bell state,

$$|\Phi_0\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{30}$$

which cannot be written in product state form.

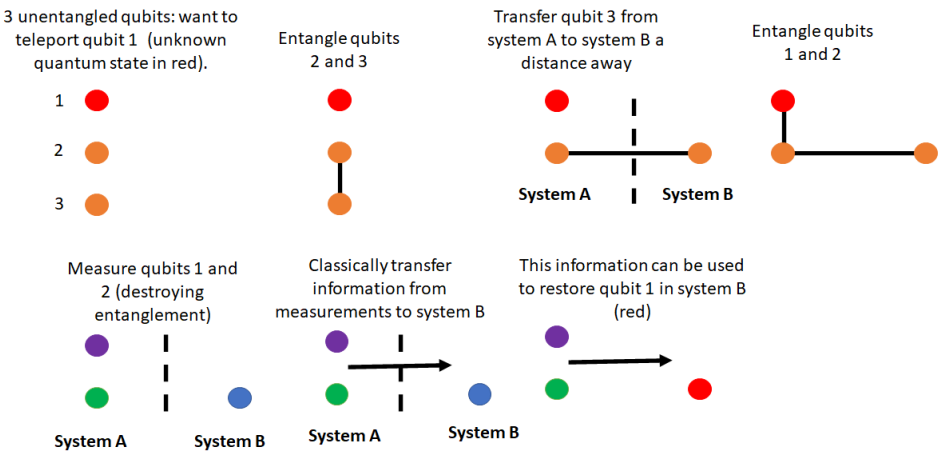

Figure 3: The quantum teleportation protocol. Different colours represent different quantum states, while solid black lines represent shared entanglement between states.

Measurement results of multiple subsystems will yield quantum correlations, which cannot be described with a classical formalism, and as described in the next chapter, these correlations can be exploited for uses in quantum communication.

Similar notions apply not just to quantum states but also to the matrices which act upon them (which describe e.g. unitary evolution or measurements). Analogously, composite matrices that can be written in the form

$$\hat{A}_{\text{product}} = \hat{A}_0 \otimes \hat{A}_1 \otimes ... \otimes \hat{A}_{n-1} \tag{31}$$

are known as *product gates*, while composite matrices that can only be written as a linear sum of product gates are called *interaction gates*. Product gates act on each subsystem independently, while interaction gates act on one subsystem conditionally upon the state of another subsystem.

Importantly, interaction gates can act upon product quantum states and evolve them into entangled states. The amount of entanglement in a quantum state is a quantifiable resource, and this can be built up through the implementation of multiple interaction gates. After successfully generating entanglement in quantum states, this can be used in quantum communication protocols.

2.3.3 Quantum teleportation

A key use of entanglement is in the quantum teleportation protocol. For a technical introduction to this effect see Appendix A. In this section, the protocol is explored intuitively, built upon ideas introduced in the previous section.

The key idea is to transfer a quantum state from one location to another, by using interaction gates, measurements and classical communication, without any physical transfer of the quantum state itself. So long as entanglement is present, this can allow quantum states to be

communicated using only classical information transfer.

The protocol starts with three qubits, qubit 1, 2 and 3. Qubit 1 is in an unknown quantum state, which should not be measured directly, otherwise measurement collapse will occur and its quantum information will be lost. The aim is to transport qubit 1 in system A to system B which is a distance away. Initially, before communication starts, qubits 2 and 3 are entangled using an interaction gate, and qubit 3 is sent from system A to system B. Following this the communication begins: qubits 1 and 2 are entangled, and subsequently measured, destroying entanglement between all three qubits, but yielding two classical measurement results in system A. Because of the nature of entanglement and the correlations it gives rise to, these measurement results can be classically communicated to system B. Once communicated, a unitary evolution, conditional on the measurements, can be applied to qubit 3 to transform it deterministically into the quantum state originally held by qubit 1. This allows quantum information to be teleported from one system to another. A diagram outlining the process is shown in figure 3.

2.4 Continuous variables

The above sections introduce qubits as 'discrete variables', in the sense that a measurement will cause a qubit to collapse into either the $|0\rangle$ or $|1\rangle$ state. However an alternative paradigm is possible, through the use of continuous variables [Andersen et al., 2010]. In this instance, rather than having two distinct measurement states, there is instead a continuous spectrum of possible outcomes, often arising from an infinite set of modes. In fact, it is typically the case that the $|0\rangle$ and $|1\rangle$ states are not physical, requiring infinite energy to create them; rather these states can only be approached as limits. Usually, continuous variable qubits are photonically implemented via the so–called 'position and momentum quadratures' of the electric field of light, which are two aspects of the field which are orthogonal to one another. This is distinct from the discrete variable case which uses the degrees of freedom of a single photon, e.g. its polarisation or path. The benefit of continuous variable encodings, compared to single photons, is that operations are deterministic, unlike in the discrete variable case where measurements give outcomes probabilistically. The key drawbacks however are that pure $|0\rangle$ and $|1\rangle$ states are not physical – and so the quality of quantum states is reduced. In addition, continuous variable states are perturbed easily by noise. The full formalism required to describe these types of quantum states are beyond the scope of this report; here we give a very brief introduction.

In this regime, one type of states corresponds to classical states produced by a laser – these are known as *coherent states*. Mathematically, coherent states are characterised by a (complex number) parameter α and are given by the formula

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,, \tag{32}$$

where $|n\rangle$ is a photon-number state of n photons. (Photon-number states are yet another type of states, where different states simply correspond to different numbers of photons; however

these states themselves are not usually considered practical for communication.). $|\alpha|^2$ gives the mean number of photons that will be detected upon measurement of a coherent state; this obeys a Poissonian probability distribution.

There is also a notion of *squeezed states*, which is an important class of quantum states that, similarly to coherent states, consist of superpositions of multiple photon numbers. Squeezed states have potential uses in quantum computation [Menicucci et al., 2006] and communication [Holevo et al., 1999]. For photonics, the variances of the two quadratures of the electric field are altered – an infinite squeezing of the position quadrature corresponds to $|0\rangle$, while infinite squeezing of the momentum quadrature represents $|1\rangle$.

While an in-depth discussion of continuous-variable quantum information is not the focus of this report, a basic notion of coherent states and squeezed states is useful in §2.4 for considering the capacities of the most 'classical-like' quantum channels.

3 The possibilities and fundamental limitations of quantum communication

In classical communication systems it is a clear what we are communicating: ordinary classical information about well-defined variables. But in the quantum case, the informational properties are not so straightforward. We must first ask: what are we actually communicating? The answer here depends on the situation. The ability to encode information in quantum systems enables the possibility of various different communication scenarios, depending on both the task at hand and the resources available. In general, quantum channels can either be used to transmit classical information (bits) or quantum information (qubits).

At present, the main interest in quantum communication as an emerging technology is in (a) the novel possibility of communicating quantum information and (b) the possibility of communicating classical information in secret. There are also theoretical arguments that suggest quantum communication systems could potentially transmit classical information with a higher capacity than purely classical systems; however at present it is not yet clear to what extent this last application will be of practical relevance in classical communication systems.

The mathematical study of the fundamental limitations of how much information can be sent through a given channel is known as Shannon theory, after its pioneer Claude Shannon, and the quantum generalisation is known as quantum Shannon theory. Recently, a second level of quantisation of Shannon theory has been proposed, where not only the information carriers can be quantum, but also the configuration of the transmission lines themselves is treated quantum mechanically, which promises new ways of achieving higher transmission rates for both classical and quantum information [Chiribella and Kristjánsson, 2019].

In this chapter, we begin by outlining the basics of communication using quantum states in practice, followed by the main communication scenarios described by quantum theory, corresponding to: classical communication, classical communication with the assistance of shared entanglement, private classical communication, and quantum communication, respectively. This is followed by examples of several paradigmatic quantum channels and their various capacities. We then briefly review some theoretical results which suggest that encoding information in quantum states could boost the ability to send classical information through quantum channels. This is followed by a discussion of the promises and limitations quantum communication networks, culminating in the quantum internet. Finally we give an outline of the recent work on quantum communication with a quantum configuration of transmission lines.

3.1 The basics of communication in practice

Consider a typical communication setting from a sender (Alice) to the receiver (Bob) via information encoded in single photons. Here we describe the main steps before and during the

communication scenario, which are summarised in the flow chart in figure 4.

The first step is encoding. Alice encodes the state of the qubit she wants to send in some degree of freedom of a photon, for example its polarisation, time-bin, frequency, angular momentum, or spatial mode. For simplicity, here we will mostly use polarisation to illustrate the main ideas; all the encoding schemes and their experimental considerations are discussed in §4.2.1. (Note also, that encoding information in light in ways other than using single photons is possible, such as using coherent states (which correspond to classical light) or squeezed states – see §2.4. However, the formalism to describe these are beyond the scope of this report and will only briefly be described when practically relevant; all the main conceptual ideas and most of the advantages of quantum communication can be illustrated with single photon encodings).

Encoding a qubit in polarisation means that each logical state is first assigned a physical polarisation state, e.g. the computational basis states are identified with the horizontal and vertical polarisation states: $|0\rangle = |H\rangle\,,\ |1\rangle = |V\rangle$. To prepare a generic quantum state

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{33}$$

requires the preparation of the photon in the corresponding polarisation state, which in general is any state on the Poincaré sphere (and thus a superposition of the horizontal and vertical states). The complex numbers α, β (with $|\alpha|^2 + |\beta|^2 = 1$) signify the relative magnitude and relative phase of the horizontal and vertical components of the polarisation. Alice is able to control the parameters α, β, for example, if she wants to send a photon with pure horizontal polarisation, she sets $\alpha = 1$, and if she wants to send an equal superposition of horizontal and vertical polarisation, she sets $\alpha = 1/\sqrt{2}$. This can be done in practice by sending the photon through a series of optical elements, such as waveplates. These parameters are directly tuned by the action of waveplates: for example, a photon with initial polarisation state $|\psi\rangle = \cos\theta\,|H\rangle + \sin\theta\,|V\rangle$ is transformed to the state $|\psi'\rangle = \cos\theta\,|H\rangle - \sin\theta\,|V\rangle$ under the action of a half-wave plate aligned with the horizontal and vertical axes.

Encoding a qubit in a spatial mode simply means that the photon is sent through one of two paths, or in some superposition of the two paths, where the first path corresponds to the logical $|0\rangle$ and the second path to logical $|1\rangle$. This is done by sending the photon through a beamsplitter, which can for example transform a photon initially on the left-hand arm $|L\rangle$ to an equal superposition of travelling through both arms $\frac{1}{\sqrt{2}}(|L\rangle + |R\rangle)$. Similarly, encoding a qubit in the time-bin degree of freedom simply means that the photon is sent at one of two possible time steps, or in some superposition of the two time steps, where the first time step corresponds to the logical $|0\rangle$ and the second time step to logical $|1\rangle$. This can be done by sending a photon through an interferometer, with arms of different lengths, such that the arrival time of the photon depends on which arm it went through. If the photon travelled in a superposition of the two arms, then it arrives at a superposition of times.

The polarisation degree of freedom of a single photon can only be used to encode a single qubit. However, multiple degrees of freedom of the same photon can be used simultaneously

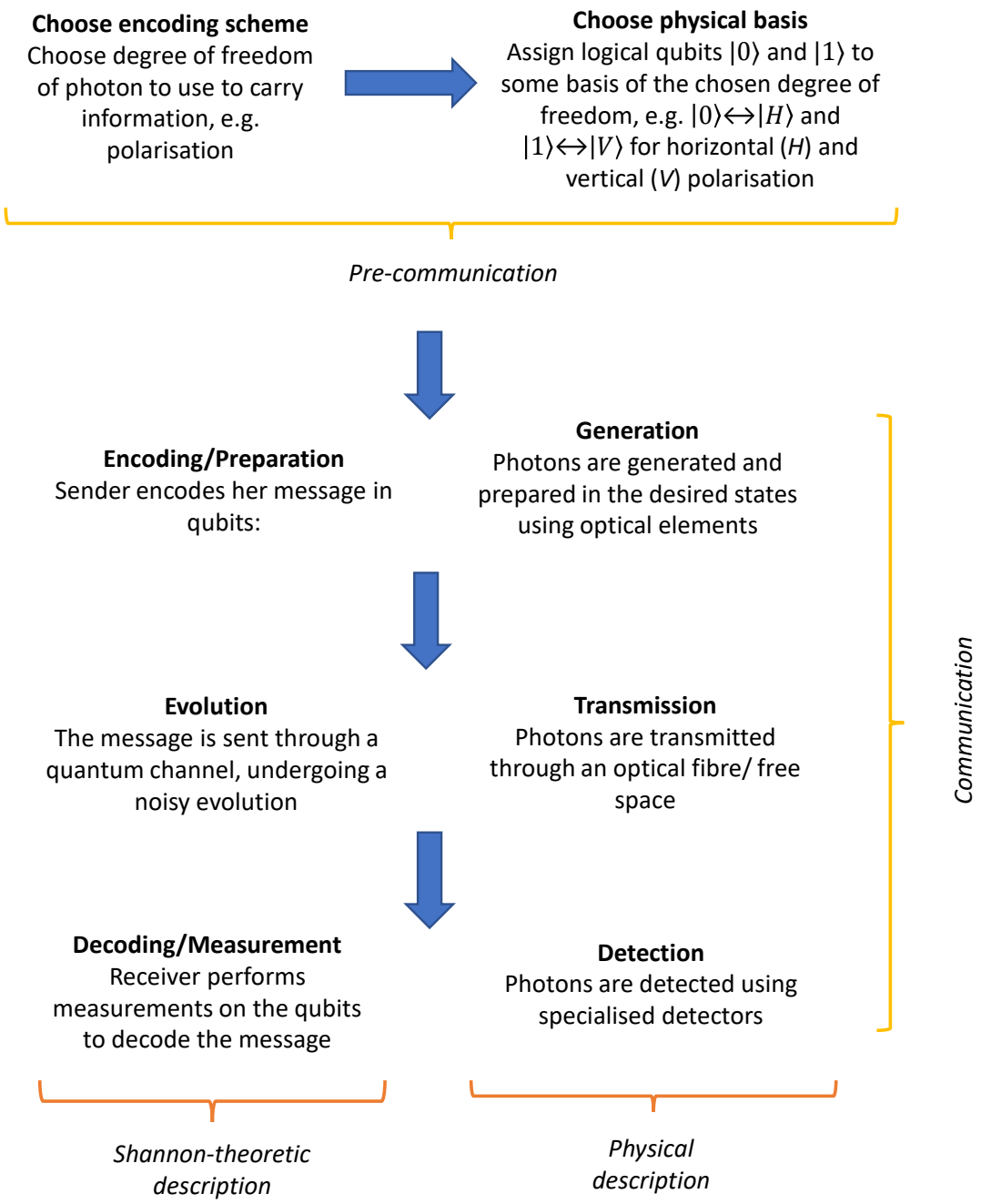

Figure 4: A flow chart showing the stages before and during communication using quantum states.

to encode multiple qubits in the same photon, for example two qubits could be encoded in a single photon by encoding one of the qubits in its polarisation and the other in its spatial mode (see also §2.2.6).

Once Alice has encoded her qubit in the photon, it is sent to Bob through an optical fibre, free space (i.e. air or vacuum, either on Earth or via a satellite), or some other medium, mathematically described by a quantum channel (§2.2.5). Finally, Bob can perform measurements on the polarisation (or other degree of freedom) to decode the logical message.

If only classical information is to be transmitted, then it is sufficient to choose two orthogonal states of the polarisation, used to encode the bits 0 and 1, respectively. These could be chosen as $|H\rangle$, $|V\rangle$ but other choices could be more appropriate for a given channel.

Just like in the classical case, in practice, quantum communication channels are subject to noise, and the task at hand is to minimise its effects to improve transmission. In the context of quantum communications, 'noise' refers to any unwanted change in the quantum state during transmission, and will be used synonymously with 'error'. (Note, that noise includes both what is known as additive noise and multiplicative noise in classical communications.) In this chapter, we are only considering the noise that is inherent in communication channels. For this type of noise, optimal encoding and decoding schemes can be designed and implemented by the communicating parties to maximise the usefulness of the channel.

An example of a noisy quantum channel is the depolarising channel which maps an input state to a randomisation of the original state and white noise. Of course, the devices used for the production and detection of photons also induce errors. These errors are typically related to the particular way in which the devices are engineered and the main challenge is to engineer less noisy devices; current progress is discussed in §4. However, when only the noise inherent in quantum channels themselves is considered, this is quantified by various types of capacities, which depend only on the channels themselves.

3.2 Communication scenarios

In classical communication, there is only one type of channel capacity C, corresponding to one type of communication. On the other hand, a quantum channel has four different capacities associated with it: 1. Classical Capacity C_{C}, 2. Entanglement-Assisted Classical Capacity C_{EA}, 3. Private Classical Capacity C_{P}, and 4. Quantum Capacity C_{Q}, corresponding to four distinct types of communication scenarios. Here we briefly describe each of these types of communication scenarios and why they are important, and conclude with a short discussion on network communication between multiple communication parties. In Appendix B these different measures of capacities are discussed in further detail, and formulas given for how to calculate them in general, whilst §3.3 gives the values of, or bounds on, the capacities for various quantum channels.

3.2.1 Classical communication between a sender and receiver

The paradigmatic communication scenario of classical Shannon theory, namely the direct communication of bits through a noisy channel between a sender (Alice) and a receiver (Bob), is also an important scenario in the quantum case. As we have seen, one qubit of information can be used as a single classical bit, when preparation and measurement are restricted to a fixed basis. This means that any quantum channel can also be used to transmit classical bits. An important point to note here is that a classical bit can be encoded in *any* qubit basis, and the basis can be chosen depending on the noise in a particular channel. For example, a bit flip channel (see §3.3.1) flips the qubits $|0\rangle \leftrightarrow |1\rangle$ with some given noise probability p, but has no effect on information encoded in the qubits $|+\rangle, |-\rangle$ (where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$).

A theoretical reason why sending classical information through quantum channels might be interesting is that entanglement between successive qubits sent through the channel may be able to enhance its communication rate [Hastings, 2009]. The idea here is the following: in a purely classical setting, all that can be sent through a bit channel is a sequence of bits. This means that the transmission rate given n uses of the channel is the same as n times the transmission rate of a single use of the channel. Strikingly, this simple intuition breaks down in the quantum case. Here, the qubits sent at successive uses of the channel can be entangled, meaning that the n entangled uses of the channel no longer factorise into n independent uses. This property of the transmission rate of quantum channels is known as superadditivity, and is quantified in the next section.

From a practical point of view, however, note that the currently known examples of quantum channels which exhibit superadditivity of the classical capacity do not correspond to those channels actually encountered in real-life communication systems. This means that it is not yet clear to what extent, if at all, encoding classical information in entangled quantum states provides a practical advantage over purely product state encodings.

Classical communication through a quantum channel is quantified by the **classical capacity of a quantum channel** C_{C}, which is defined as the maximum number of bits that can be transmitted through the channel, per channel use, in the asymptotic limit of infinitely many uses. This is quantified mathematically in Appendix B.2. Here, and in the rest of this report, a *use* of a channel refers to a single instance of sending a symbol through a channel – in the case of 2-dimensional channels (as focused on here) this mean sending a single bit or qubit. So, the classical capacity reduces to the ratio of the number of message bits sent vs the number of message bits received, in the limit of being able to send an infinitely large number of bits. If superadditivity were not present, then the limit of sending infinitely many bits would not be necessary.

In §3.3, the classical capacity is evaluated for the various common examples of quantum channels discussed in that section. Note that for qubit channels (i.e. where the message is two-dimensional), the maximum classical capacity is 1 – corresponding to one bit being received per message bit sent.

3.2.2 Classical communication between a sender and receiver assisted by shared entanglement

The transmission of classical information can also be enhanced by allowing shared entanglement between the communicating parties [Bennett et al., 1999]. This means that prior to the communication scenario, Alice and Bob first generate a bipartite entangled state, and each take one half of it into their possession. For an ideal noiseless communication channel, if Alice is able to transmit n bits through the channel on its own, then she can transmit $2n$ bits through the channel when Alice and Bob have access to n shared entangled states. The paradigmatic protocol which achieves this is called superdense coding [Bennett and Wiesner, 1992] and is discussed in §5.3.

In practice, however, the distribution of an entangled state between distant parties is usually a much more difficult task than transmitting classical information in the first place, so this scheme is unlikely to have practical utility for all forms standard communication of classical information across large distances, but may be useful in various specific scenarios where pre-sharing entanglement at an earlier time is easier than sending classical bits at the time of communication. With current photonic technology, it is moreover very difficult to maintain entanglement between distant parties over the timescale required to send photons through the channel. Therefore, the advantages of shared entanglement for classical communication can only be realised when *quantum memories* become available – that is, technology for storing quantum states (see §3.5.4).

Classical communication through a quantum channel assisted by shared entanglement is quantified by the **entanglement-assisted classical capacity** of the channel C_{EA}, which is defined as the maximum number of bits that can be transmitted through the channel, per channel use, in the asymptotic limit of infinitely many uses, assuming an unlimited number of entangled states between the sender and receiver. This is quantified mathematically in Appendix B.3. The entanglement-assisted classical capacity does not exhibit superadditivity, so the limit of sending infinitely many bits is not necessary [Wilde, 2013]. In §3.3, the entanglement-assisted classical capacity is evaluated for the various common examples of quantum channels discussed in that section.

3.2.3 Private communication between a sender and receiver

The laws of quantum theory enable not only the quantification of how many bits of information can be transmitted from the sender to the receiver, but also how many bits can be transmitted privately between them, inaccessible to an eavesdropper. This is known as the communication of private classical information; the privacy is guaranteed by the laws of physics unlike current cryptographic protocols which rely on assumptions about the computational power of the eavesdropper. The No Cloning Theorem dictates that a generic quantum state cannot be cloned, that is, there does not exist any physically allowed quantum operation that takes any quantum state $|\psi\rangle$ to two copies of the state $|\psi\rangle \otimes |\psi\rangle$. This means that a generic quantum state cannot be simultaneously distributed to more than one party. Therefore, an eavesdropper (Eve) cannot

intercept a transmission line and retrieve the information without in some way disturbing the transmission to Bob. This is the intuition behind the notion of private information. By appropriate encoding of classical information into quantum states, Alice and Bob can establish a fundamental bound on the amount of information that Eve can intercept between them. The amount of information Alice and Bob can communicate in secret is known as the *private information*. The simplest example of a task which utilises the private information is generating a secret key between Alice and Bob for quantum key distribution (QKD). However, note that QKD and the associated classical communication of the encrypted information is only one specific way in which private information can be transmitted. The ability to quantify the private information of any quantum channel enables a fundamentally quantifiable bound of the security through any given transmission link between a sender and receiver, involving only the channel itself without necessarily the need for key distribution.

At this point the reader may wonder why quantum-level security is necessary at present. The reason is the following: Current cryptographic protocols for transmitting and storing information securely rely on assumptions about the difficulty of performing certain computational tasks. For example, RSA encryption relies on the practical impossibility of factoring large numbers. With the current technological capabilities, these assumptions are well justified, however, the advent of quantum computers poses a threat to the guarantee of long-term cryptographic security. For example, an implementation of Shor's algorithm would be able to break RSA encryption [Nielsen and Chuang, 2000]. The most imminent threat is that of 'intercept now, decrypt later' attacks. Health, intelligence and military data typically has a timescale of x years for which it is required to remain confidential. Then, if it takes z years to build a quantum computer capable of breaking current security, and y years to build a post-quantum secure infrastructure resistant to quantum attacks, then security is compromised if $z < x + y$ [Stebila et al., 2009]. Taking an individual's private health data as an example, this may be required to remain confidential for at least two or three generations ($\sim$100 years). This means that as long as a quantum computer is commercialised within 100 years, this health data is *already* compromised.

Private classical communication through a quantum channel is quantified by the **private classical capacity** of the channel C_{P}, which is defined as the maximum number of bits that can be transmitted through the channel, per channel use, in the asymptotic limit of infinitely many uses, such that the transmitted bits are inaccessible to anyone else. This is quantified mathematically in Appendix B.4. In §3.3, the private classical capacity is evaluated for the various common examples of quantum channels discussed in that section.

3.2.4 Quantum communication between a sender and receiver

In addition to classical bits, quantum channels can also directly transfer quantum states (i.e. qubits, in the case of 2-d systems) between a sender and receiver. In a future where multiple quantum computers at different locations need to share information to work together, the reliable communication of qubits between them will be of paramount importance. Moreover,

the possibility of secure quantum key distribution relies on the existence of reliable quantum communication channels. In these cases, Alice prepares a qubit in any of its possible states (any point on the Bloch ball), and aims to send the whole qubit itself to Bob, not only classical information about it. This means that Bob will be able to use the qubit directly in computational tasks without assuming that the state has collapsed to a given basis. Crucially, this also means that if the initial qubit Alice sent was entangled with another qubit in her lab, then the entanglement is preserved after the qubit is transferred to Bob. This enables Alice and Bob to carry out quantum computational tasks which require entanglement between distant parties.

Key use cases where quantum communication is required are e.g. distributed quantum computing, quantum cloud computing and ultraprecise GPS, which at large scales will require a global network of interconnected quantum computers, known as the **quantum internet**.

The transmission of quantum information through a noisy quantum channel can be enhanced by allowing access to a noiseless classical channel [Bennett et al., 1996], in addition to the noisy quantum channel used to send the quantum information of interest. In practice, this is a common scenario, since current technology can easily produce classical transmission lines with near-perfect rates, whilst the transmission of quantum information is much more difficult.

Remarkably, two uses of a classical channel together with shared entanglement can even reproduce the transmission of a quantum state, without using a quantum channel to physically transmit the state. That is, in addition to the possibility of directly sending a qubit from Alice to Bob, it is also possible to achieve quantum communication using quantum teleportation. As seen in §2.3.3, on teleportation, the quantum communication of a single qubit is possible using (a) a shared entangled state between the sender and receiver and (b) two classical bits that can be communicated noiselessly, without actually physically transmitting the original qubit system itself. This means that the task of quantum communication of an arbitrary state $|\psi\rangle$ can be reduced to the task transmitting half of a fixed entangled state from Alice to Bob, assuming that classical communication is available (e.g. using conventional communication systems).

Quantum communication through a quantum channel is quantified by the **quantum capacity** of the channel C_{Q}, which is defined as the maximum number of qubits that can be transmitted through the channel, per channel use, in the asymptotic limit of infinitely many uses. Note, that like the classical capacity, the quantum capacity is superadditive in general. This is quantified mathematically in Appendix B.5. In §3.3, the quantum capacity is evaluated for the various common examples of quantum channels discussed in that section. Note that for qubit channels (i.e. where the message is two-dimensional), the maximum quantum capacity is 1 – corresponding to one qubit being received per message qubit sent.

3.2.5 Network communication between multiple parties

In the future, we would expect multiple communicating parties to be connected by a network of multiple quantum communication channels – with the ultimate goal being a quantum

internet. This introduces new questions about the most efficient way to design the network architecture and how to correct errors at intermediate nodes, discussed in depth in §3.5.

As special cases of network communication, one can consider a multiple access channel, which has multiple senders and a single receiver, as well as a quantum broadcast channel, which has a single sender and multiple receivers. One can also consider a quantum interference channel, which has multiple senders and multiple receivers, where different choices of pairs of senders and receivers can communicate. The different types of communication scenarios described above can all be applied to these more elaborate types of channels, however, they have additional subtleties compared to their classical counterparts, which are only recently being explored in the theoretical literature [Wilde, 2013].

3.2.6 Summary and comparison of communication scenarios and channel capacities

Type of information	**Transmitted via**	**Information measure**	**Usefulness?**
Classical information	classical channel	channel capacity C	all current technology: optical fibres, radio transmission, wifi, 4G, 5G, etc.
Classical information	quantum channel	classical capacity C_{C}	potentially higher communication rates
Classical information	quantum channel and shared entanglement	entanglement-assisted classical capacity C_{EA}	superdense coding
Private (classical) information	quantum channel	private (classical) capacity C_{P}	secure communication, e.g. quantum key distribution (QKD)
Quantum information	quantum channel	quantum capacity C_{Q}	quantum internet, e.g. distributed quantum computing, quantum cloud computing, ultraprecise GPS, etc.

An important point to note is that quantum communication implies the possibility of private communication, which in turn implies the possibility of classical communication. Therefore, we have the following inequalities [Li et al., 2009] for any given quantum channel $\mathcal{N}$:

$$C_{\mathrm{C}}(\mathcal{N}) \geq C_{\mathrm{P}}(\mathcal{N}) \geq C_{\mathrm{Q}}(\mathcal{N}). \tag{34}$$

Similarly, classical communication implies the possibility of entanglement-assisted classical communication, which means that

$$C_{\mathrm{EA}}(\mathcal{N}) \geq C_{\mathrm{C}}(\mathcal{N}). \tag{35}$$

3.3 Examples of noisy discrete quantum communication channels and their various capacities

3.3.1 Bit-flip channel

One of the simplest examples of a quantum channel is the quantum bit-flip channel, which takes $|0\rangle$ to $|1\rangle$ with an error probability p, and vice versa. This is the quantum analogue of the classical binary symmetric channel, which flips the bits 0 or 1 with probability p. Mathematically, the quantum bit-flip channel acting on any input quantum state ρ is given by

$$\mathcal{N}_{\mathrm{bit-flip}}(\rho) = (1-p)\rho + X\rho X, \tag{36}$$

where X is the Pauli X matrix (see eq. (8)) which swaps $|0\rangle$ and $|1\rangle$. The Kraus operators (§2.2.5) of the channel are $K_0 = \sqrt{p}I, K_1 = \sqrt{1-p}X$.

The quantum bit-flip channel acts as the classical binary symmetric channel when the input states are restricted to the *computational basis states* $|0\rangle$ and $|1\rangle$. However, it acts in non-trivial ways when the input states are more general quantum states. In particular, when the input states are the *Fourier basis states*

$$|\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) \tag{37}$$

the bit flip channel acts as the identity channel(!) This highlights a fundamental property of the resistance of quantum states to noise: even if noise acts on a particular basis of states, there can exist a different basis of states for which a channel is less noisy (or in this case, noiseless).

Now, let us consider the various capacities of the bit-flip channel. The channel capacity of the classical binary symmetric channel is given by

$$C(p) = 1 - H_2(p) \tag{38}$$

bits per channel use, where $H_2(p)$ is the binary entropy function of probability p:

$$H_2(p) = -p\log_2 p - (1-p)\log_2(1-p) \tag{39}$$

In the quantum case, however, the classical capacity of the quantum bit-flip channel is simply

$$C_{\mathrm{C}}(\mathcal{N}_{\mathrm{bit-flip}}) = 1 \tag{40}$$

bit per channel use, as seen above, independent of the error probability p, because quantum allows for the additional freedom to optimise over the input states, in this case choosing the Fourier basis states $|\pm\rangle$ instead of the computational basis states $|0\rangle$ and $|1\rangle$.

The entanglement-assisted classical capacity of the quantum bit-flip channel is

$$C_{\mathrm{EA}}(\mathcal{N}_{\mathrm{bit-flip}}) = 2 - H_2(p) \tag{41}$$

bits per channel use, which recovers the dependence on p as in the classical case [Raina and Srinivasa, 2014]. This is always larger than or equal to the classical capacity, and up to one bit larger, showcasing the advantage of entanglement-assistance.

The quantum capacity of the quantum bit-flip channel is

$$C_{\mathrm{Q}}(\mathcal{N}_{\mathrm{bit-flip}}) = 1 - H_2(p) \tag{42}$$

qubits per channel use (which interestingly is identical to the channel capacity of the classical binary symmetric channel) [Wilde, 2013].

3.3.2 Depolarising channel

An example of a common physical process which results in errors hindering the transfer of classical information is the *depolarising error*. A quantum channel which induces a depolarising error is called a depolarising channel, here denoted $\mathcal{N}_{\mathrm{dep}}$. Given an input state ρ, the depolarising channel returns the original state with probability $(1-p)$, and replaces it with the maximally mixed state (i.e. white noise) with probability p. In equations,

$$\mathcal{N}_{\mathrm{dep}}(\rho) = (1-p)\rho + p\frac{I}{d}, \tag{43}$$

where we recall that the maximally mixed state is given by the identity matrix I divided by the dimension of the system d.

The depolarising error affects both classical and quantum states in the same way. Note that since quantum information is a strictly stronger type of information than classical information (classical information is essentially just quantum information restricted to a fixed basis), then any error which affects classical information transfer affects quantum information transfer at least as much.

The depolarising channel can arise via a randomisation over a (orthogonal) set of unitary matrices. For example, for qubits ($d = 2$),

$$\mathcal{N}_{\mathrm{dep}}(\rho) = \left(1 - \frac{3p}{4}\right)\rho + \frac{p}{4}(X\rho X + Y\rho Y + Z\rho Z), \tag{44}$$

where X, Y, Z are the Pauli matrices (eq. (8)).

The classical capacity of the depolarising channel does not exhibit superadditivity, and can therefore be computed exactly as

$$C(\mathcal{N}_{\mathrm{dep}}) = \log d - H_{\min}(\mathcal{N}_{\mathrm{dep}}) \tag{45}$$

bits per channel use, where

$$H_{\min}(\mathcal{N}_{\mathrm{dep}}) = -(1-p+p/d)\log(1-p+p/d) - (d-1)(p/d)\log(p/d) \tag{46}$$

is a quantity known as the minimum output entropy of the channel [King, 2003]. The entanglement-assisted classical capacity of the depolarising channel is given by

$$C_{\mathrm{EA}}(\mathcal{N}_{\mathrm{dep}}) = 2\log d - H_{d^2}\left(1 - p\frac{d^2-1}{d^2}\right) \tag{47}$$

bits per channel use, where

$$H_d(x) = -x\log x - (1-x)\log\left(\frac{1-x}{d-1}\right) \tag{48}$$

[Bennett et al., 1999].

The quantum capacity of the depolarising channel has not yet been computed analytically; the difficulty is due to the fact that the quantum capacity is superadditive. However, upper and lower bounds to the quantum capacity have been found with increasing tightness; in 2020 a new upper bound was published as

$$C_{\mathrm{Q}}(\mathcal{N}_{\mathrm{dep}}) \leq \log d + \eta\left(\frac{1}{2}\right) - \eta\left(\frac{1}{2} - \frac{(d^2-1)p}{d^2}\right) - (d^2-1)\eta\left(\frac{p}{d^2}\right) \tag{49}$$

qubits per channel use, where $\eta(x) = -x\log x$ [Fanizza et al., 2020]. The lower bound is given by

$$C_{\mathrm{Q}}(\mathcal{N}_{\mathrm{dep}}) \geq \log d - \eta\left(1 - p + \frac{p}{d^2}\right) - (d^2-1)\eta\left(\frac{p}{d^2}\right) \tag{50}$$

qubits per channel use.

3.3.3 Dephasing channel

The paradigmatic error which affects the communication of quantum information, but not classical information, is the *dephasing error*. The dephasing error collapses a quantum state into a given classical basis, thus losing its essential quantum properties. Dephasing occurs naturally in most quantum systems due to their interaction with the environment and, ultimately, is the reason why the world around us appears classical. Mathematically, a dephasing channel $\mathcal{N}_{\mathrm{deph}}$ has the following form:

$$\mathcal{N}_{\mathrm{deph}}(\rho) = (1-p)\rho + p\sum_{i}^{d} |i\rangle\langle i|\,\rho\,|i\rangle\langle i|\,, \tag{51}$$

where $|i\rangle$ are the basis vectors of the information-carrying system (of dimension d).

As an example, consider the completely dephasing channel ($p = 1$), acting on the equal superposition of the computational basis states $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. The input density matrix is

$$|+\rangle\langle+| = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|0\rangle\langle 1| + \frac{1}{2}|1\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\,, \tag{52}$$

and the output density matrix is given by

$$\mathcal{N}^{p=1}_{\text{deph}}(|+\rangle\langle+|) = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\,. \tag{53}$$

As we can see, the completely dephasing channel has destroyed the off-diagonal elements, corresponding to the quantum coherences. However, we have that

$$\mathcal{N}^{p=1}_{\text{deph}}(|0\rangle\langle 0|) = |0\rangle\langle 0| \tag{54}$$
$$\mathcal{N}^{p=1}_{\text{deph}}(|1\rangle\langle 1|) = |1\rangle\langle 1|\,, \tag{55}$$

so classical bits can still be sent noiselessly through the channel.

The dephasing channel is in fact mathematically equivalent to the quantum bit-flip channel discussed above, in the sense that it acts on the computational basis states $\{|0\rangle\,, |1\rangle\}$ in the same way that the quantum bit-flip channel acts on the Fourier basis states $\{|+\rangle\,, |-\rangle\}$, and vice versa. Graphically, the dephasing channel moves any state on the Bloch ball (§2.1.3) towards the z-axis (between the poles), whilst the quantum bit-flip channel moves any state on the Bloch ball towards the x-axis (parallel to the equator). Consequently, the various capacities of the dephasing channel are identical to those of the quantum bit-flip channel.

3.3.4 Erasure (loss) channel

The classical erasure channel transmits a $d-$dimensional message correctly with some probability $(1-\gamma)$, and transmits an error state with probability γ. For bits ($d=2$), the channel is commonly known as the binary erasure channel.

The quantum erasure channel channel generalises this to the quantum case, for any ($d-$dimensional) message system. It represents a simple model of photonic loss, which is present in all optical fibres and free space. Let the information be encoded in any internal degree of freedom of a single photon, e.g. a polarisation qubit ρ (in which case $d=2$). The erasure channel destroys the photon all together with probability γ, leaving the vacuum state $|\text{vac}\rangle$, which corresponds the absence of a photon – note that in quantum theory even the absence of a particle is still a quantum state. Mathematically we write,

$$\mathcal{N}_{\text{erasure}}(\rho) = (1-\gamma)\rho + \gamma\,|\text{vac}\rangle\langle\text{vac}|\,. \tag{56}$$

The classical erasure channel has channel capacity

$$C(\gamma) = (1-\gamma)\log d \tag{57}$$

bits per channel use. The quantum erasure channel also has classical capacity

$$C_{\text{C}}(\mathcal{N}_{\text{erasure}}) = (1-\gamma)\log d \tag{58}$$

bits per channel use. Its entanglement-assisted classical capacity is twice that, namely

$$C_{\mathrm{EA}}(\mathcal{N}_{\mathrm{erasure}}) = 2(1-\gamma)\log d \tag{59}$$

bits per channel use [Bennett et al., 1999]. The quantum capacity of the quantum erasure channel is given by

$$C_{\mathrm{Q}}(\mathcal{N}_{\mathrm{erasure}}) = \begin{cases} (1-2\gamma)\log d & \text{for } 0 \leq \gamma \leq \frac{1}{2} \\ 0 & \text{for } \frac{1}{2} < \gamma \leq 1 \end{cases} \tag{60}$$

qubits per channel use [Wilde, 2013].

3.3.5 Summary of the various capacities of important quantum channels

Table 1 summarises the various capacities of the quantum channels considered in this section, and also includes the continuous-variable quantum channels considered in the next section. Some of the expressions for the capacities are given in terms of certain entropic quantities, which are given again below:

$$\begin{aligned} H_2(p) &= -p\log_2 p - (1-p)\log_2(1-p) \\ H_{\min}(p,d) &= -(1-p+p/d)\log(1-p+p/d) - (d-1)(p/d)\log(p/d) \\ H_d(x) &= -x\log x - (1-x)\log\left(\frac{1-x}{d-1}\right) \\ g(x) &= (x+1)\log_2(x+1) - x\log_2 x \end{aligned}$$

3.4 Comparison of classical and quantum methods for classical communication through examples of continuous-variable channels

So far, all of the examples of quantum communication have been about qubits encoded in the *discrete* states of single photons travelling through quantum channels with *discrete* noise models. However, a reader familiar with classical communication systems might wonder how this can be directly related to the classical case of encoding information in the continuous classical states of light.

An important point to note in order to understand this difference is that in the classical case, discrete channels, such as the binary symmetric channel, are typically used as textbook illustrations, whilst practical scenarios involve sending information through channels with continuous parameters, such as the additive Gaussian white noise (AGWN) channel [Cover and Thomas, 2006]. On the other hand, in the quantum case, it is often most practical to encode information in discrete states of single photons (e.g. polarisation), in which case we have a discrete system, and therefore the noise models will also be discrete. This means that realistic noise models for single-photon communication consist of discrete channels, such as those

Table 1: Table summarising the various capacities of the example types of quantum channels considered in §3.3–3.4

Type of channel & parameters	**Classical capacity**	**Entanglement-assisted classical capacity**	**Quantum capacity**	**Classical capacity of analogous classical channel**
Bit-flip channel / dephasing channel (error prob. p)	1	$2 - H_2(p)$	$1 - H_2(p)$	$1 - H_2(p)$
Depolarising channel (error prob. p, message dimension d)	$\log d - H_{\min}(p, d)$	$2\log d - H_{d^2}\left(1 - p\frac{d^2-1}{d^2}\right)$	$\log d - \eta\left(1 - p + \frac{p}{d^2}\right) - (d^2-1)\eta\left(\frac{p}{d^2}\right) \leq C_C \leq \log d + \eta\left(\frac{1}{2}\right) - \eta\left(\frac{1}{2} - \frac{(d^2-1)p}{d^2}\right) - (d^2-1)\eta\left(\frac{p}{d^2}\right)$ (61)	N/A
Erasure channel (erasure prob. γ)	$(1-\gamma)\log d$	$2(1-\gamma)\log d$	$\begin{cases} (1-2\gamma)\log d & \text{for } 0 \leq \gamma \leq \frac{1}{2} \\ 0 & \text{for } \frac{1}{2} < \gamma \leq 1 \end{cases}$ (62)	$(1-\gamma)\log d$
Gaussian pure loss channel (loss prob. $(1-\eta)$, average photon number N_S)	$g(\eta N_S)$	N/A	N/A	N/A
Quantum AGWN (average photon number N_S, Gaussian error variance M)	$g(N_S + M) - g(M)$	N/A	N/A	$\frac{1}{2}\log\left(1 + \frac{P}{M}\right)$

discussed in the previous section. Single photon states do not exist in classical physics, and therefore it is not possible to construct a direct comparison with the classical case for these channels. As done in the previous section, it is therefore only possible to compare the discrete quantum channels with their classical analogues, such as the quantum bit-flip channel with the classical binary symmetric channel; however, this comparison is perhaps not of great practical value since the classical discrete channels are not widely used in practical scenarios.

In order to make a more useful comparison between classical and quantum communication, we can also consider continuous quantum channels, where information is encoded not in single photons, but in continuous-variable quantum states of light (see §2.4). One such encoding is coherent states, which corresponds to classical light emitted from a laser. Another example is squeezed states, which are non-classical states. Continuous-variable quantum communication has both pros and cons compared to single-photon communication, which are touched on in §2.4.

For continuous-variable quantum channels, similarly to continuous classical channels, since there is no a priori limit on the size of a codeword, the capacity could be infinite without further restriction. Classically, a common constraint on the input of the channel is a fixed average input energy or power, for example, for a codeword $(x_1, x_2, \ldots, x_n)$, the requirement could be that

$$\frac{1}{n}\sum_{i=0}^{n} x_i^2 \leq P, \tag{63}$$

for some power P [Cover and Thomas, 2006]. Similarly, in the quantum case, an energy constraint could be

$$\hbar\omega_k N_k \leq E, \tag{64}$$

where $\hbar\omega_k$ is the energy of a single photon in the given mode k ($\hbar$ is the reduced Plank's constant and ω_k is the frequency of the mode k), and N_k is the average number of photons in the mode k [Giovannetti et al., 2004]. (This is assuming only a single mode; for multi-mode channels this generalises to a sum over k.)

For the purpose of sending classical information through continuous-variable quantum channels, one can ask what type of quantum states can be used to encode information in order to achieve the capacity of the channel, e.g. coherent states (which can be realised classically) or squeezed states (which cannot be realised classically). A similar question can be asked about decoding the information at the receiver's end. Classically, one can consider three types of detection methods: direct detection, homodyne detection, and heterodyne detection [Shapiro, 2009]. Quantum theory, however, allows for more general forms of detection, involving joint measurements on multiple (possibly entangled) quantum states. However, note that these measurements are not all implementable with current technology, so their potential advantages will only become clear in the long term [Shapiro, 2009]. Given a quantum channel with a known capacity, one can therefore ask whether non-classical detection methods are necessary to achieve the capacity.

Here we consider three examples of continuous-variable quantum optical channels with

Gaussian noise: a pure loss channel (where the capacity has a simple expression), a quantum analogue of the additive Gaussian white noise (AGWN) channel, and a realistic model of a line-of-sight free-space channel. The main result for all three channels is that their classical capacity can be achieved using coherent-state encodings (i.e. quantum-specific states such as squeezed states do not give an advantage) but requires non-classical decoding methods. That is, **quantum detection methods give a capacity advantage over classical detection methods**. In addition to direct classical communication, continuous-variable quantum systems can also be used to perform entanglement-assisted classical communication. In these cases, the use of squeezed states can be used to achieve entanglement-assisted classical capacities that exceed the corresponding classical capacities, but only under the assumption that the energy cost of pre-sharing entanglement between the sender and receiver is neglected – which is not necessarily a justified assumption [Shapiro, 2021]. In the following, we will focus on direct classical communication.

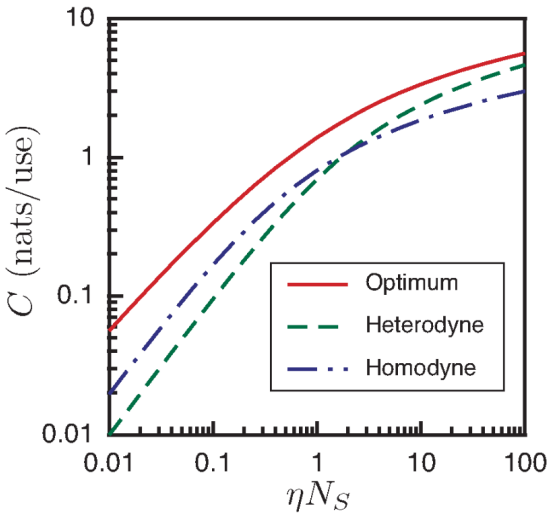

Figure 5: Classical capacity of a quantum Gaussian pure loss channel with coherent state encodings, as a function of the parameter ηN_S, where η is the channel transmissivity and N_S is the average photon number of the transmitter. The solid curve shows the optimum capacity found mathematically, while the dashed and dot-dashed curves show the capacity when detection is restricted to (classical) heterodyne and homodyne detection, respectively. Whenever the red curve is above the other two, quantum detection methods exhibit a capacity advantage over classical ones. The largest quantum advantage is found at low photon numbers: for $\eta N_S = 0.01$ the capacity achievable using quantum detection methods is approximately **2.5 times larger** than that achievable using classical detection methods. Figure taken from [Shapiro, 2009].

3.4.1 Gaussian pure loss channel

The Gaussian pure loss channel $\mathcal{N}_{\text{loss}}$ is a continuous-variable channel where a photon is lost with probability $(1-\eta)$. We assume an energy constraint such that the average photon number

is at most a fixed value N_S. The classical capacity of this channel was found to be

$$C(\mathcal{N}_{\text{loss}}) = g(\eta N_S) \tag{65}$$

nats per channel use, with $0 \leq \eta \leq 1$, where

$$g(x) := (x+1)\log_2(x+1) - x\log_2 x \tag{66}$$

[Giovannetti et al., 2004, Shapiro, 2009].

For the Gaussian pure loss channel, it was found that the capacity can be achieved with classical coherent states. This means that encoding in quantum-specific states is not necessary to achieve the capacity. However the optimal decoding strategy requires joint quantum measurements on multiple output states, which cannot be implemented via standard classical measurement techniques. In particular, the classical capacity of the channel when coherent-state encoding is used together with either homodyne or heterodyne detection (classically possible) is given by

$$C_{\text{hom}}(\mathcal{N}_{\text{loss}}) = \frac{\ln(1+4\eta N_S)}{2} \tag{67}$$

nats per channel use, and

$$C_{\text{het}}(\mathcal{N}_{\text{loss}}) = \ln(1+\eta N_S) \tag{68}$$

nats per channel use.

Figure 5 shows the achievable capacity for the optimal decoding strategy (corresponding to eq. (65)) and (classical) homodyne and heterodyne detection (corresponding to eqs. (67) and (68)) [Shapiro, 2009]. It can be seen that in the limit of very large numbers of photons, classical heterodyne detection is asymptotically optimal [Giovannetti et al., 2004], whilst non-classical detection methods are needed to achieve the full capacity in all the other regimes.

3.4.2 Quantum analogue of the additive Gaussian white noise channel

We now consider a quantum description of a classical noise channel which can be seen as a quantum analogue of the additive Gaussian white noise (AGWN) channel. This consists of Gaussian white noise on the (complex-valued) parameter α that characterises coherent states (see §2.4), thus mapping an input coherent state to another coherent state, with the difference between to two states following a Gaussian distribution. Formally, the channel is given by

$$\mathcal{N}_{\text{gauss}}(\rho) = \int \mathrm{d}^2\alpha \frac{\exp(-|\alpha|^2/M)}{\pi M} D(\alpha)\rho D^\dagger(\alpha), \tag{69}$$

where $D(\alpha)$ is the operator which maps a coherent state $|\alpha_0\rangle$ to $|\alpha_0+\alpha\rangle$ and $M \in \mathbb{R}$ is the variance.

The classical capacity of this channel is lower bounded by the achievable rate

$$R = g(N_S + M) - g(M) \tag{70}$$

nats per channel use, which is achievable using (classical) coherent-state encodings, and is higher than the capacity achievable using classical detection methods [Shapiro, 2009]. That is, non-classical (i.e. quantum) measurement techniques give an advantage for the classical capacity.

This can be compared with the classical AGWN channel with power constraint P (analogous to N_S) and variance M, where the channel capacity is given by

$$C = \frac{1}{2}\log\left(1 + \frac{P}{M}\right) \tag{71}$$

bits per channel use [Cover and Thomas, 2006].

3.4.3 Line-of-sight free-space channel

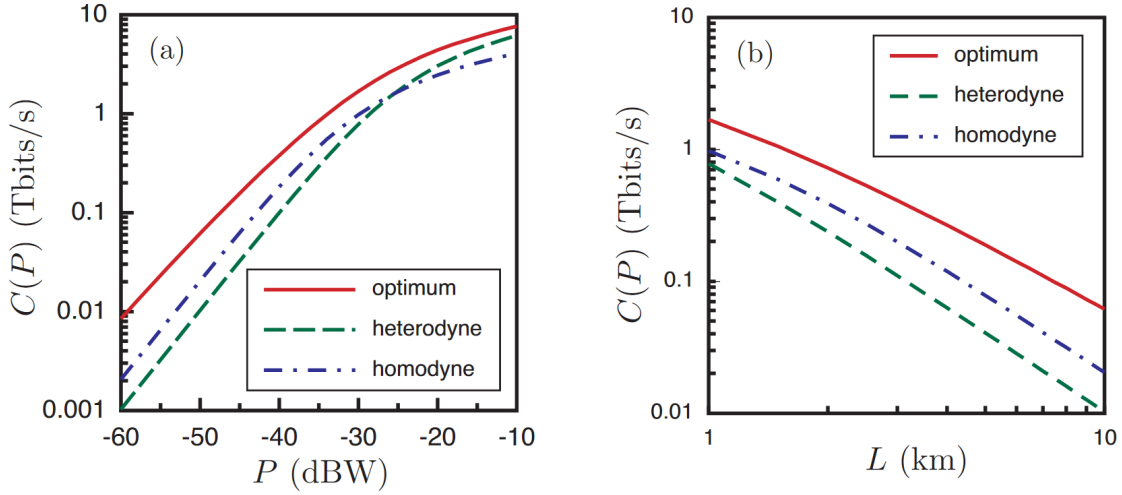

Figure 6: Classical capacity of a quantum line-of-sight free-space channel (narrowband 1.55μm wavelength channel), as a function of (a) average transmitter power P and (b) path length L. For (a), path length is taken as L =1km, and for (b), P =1 mW. The solid curve shows the optimum capacity found mathematically, while the dashed and dot-dashed curves show the capacity when detection is restricted to heterodyne and homodyne detection, respectively. Whenever the red curve is above the other two, quantum detection methods exhibit a capacity advantage over classical ones. The largest quantum advantage is found at low power: for $P = -60\text{dBW}$ the capacity achievable using quantum detection methods is approximately **4 times larger** than that achievable using classical detection methods. Figure taken from [Shapiro et al., 2005].

The realistic model of a line-of-sight free-space channel, whose detailed description and parmeterisation is beyond the scope of this report, was found to exhibit similar properties to the simplified model of a pure-loss channel and the quantum analogue of the AGWN channel. Again, the optimal decoding strategy involves non-classical methods. For the choice of parameters in [Shapiro et al., 2005], Figure 6 shows how the optimal decoding strategy compares to homodyne and heterodyne detection for the capacity against (a) average transmitter power and (b) path length.

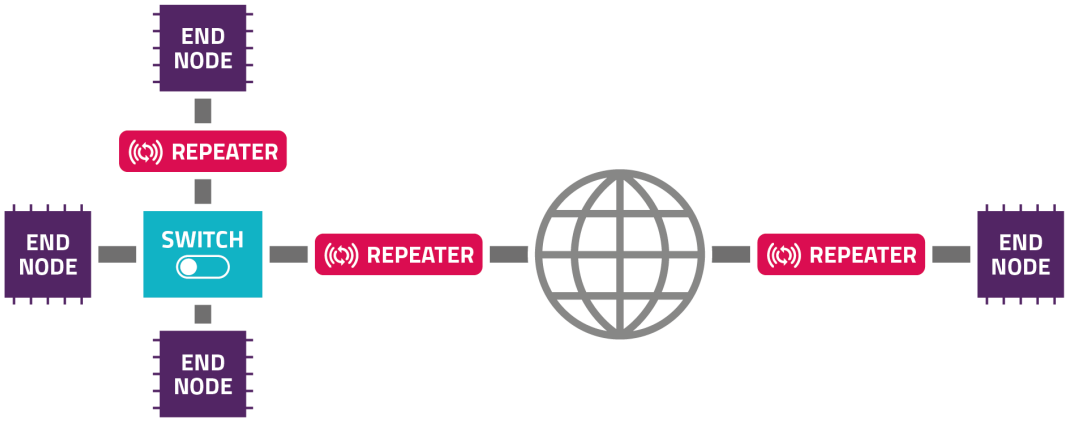

Figure 7: A schematic diagram of a worldwide quantum communication network. The end nodes are connected via quantum channels (grey cylinders) and repeaters. A switch controls which end nodes to transmit to.

3.5 Quantum communication networks: towards a quantum internet

The ultimate application of quantum communication is to build a quantum internet, securely connecting quantum processors across the world [Wehner et al., 2018]. The first step towards such a feat is to construct a quantum network, which could be at a metropolitan scale at first, extending to worldwide satellite communication at later stages.

Quantum networks enable the possibility of sending quantum information between distant parties, for example for secure quantum key distribution, or for the transfer of quantum data from experimental qubit sources to the processors that will be using them. Quantum networks are the backbone of distributed quantum computing, connecting multiple small-scale quantum processors to form an effective larger and more powerful quantum computer. This could provide a solution to one of the biggest challenges in the practical implementation of quantum computing, namely, scaling up the number of qubits. Moreover, there are problems in distributed systems which can be solved more efficiently using networks of quantum computers than classical ones [Wehner et al., 2018]. A quantum internet could also be used for quantum cloud computing, creating a quantum cloud from a network of locally hosted processors, which can be accessed by distant users in a similar way to classical cloud computing [Caleffi et al., 2018], as well as enable the possibility of a whole host of other applications, such as ultra precise GPS and clock synchronisation. These use-cases are outlined in §3.5.5.

A roadmap for the stages in the development of quantum communication networks leading up to a quantum internet is given in §6.2; more detailed discussion on the outlooks and motivations is given in [Wehner et al., 2018].

3.5.1 Structure of a network

A quantum network consists of a set of end nodes at various locations, connected via quantum communication channels, for example optical fibres. In order to allow for long-distance com-

munication, the communication channels are connected via quantum repeaters (see below). Figure 7 illustrates a basic quantum network. The implementation of the communication channels usually consists of transmitting quantum particles directly between the nodes, most commonly photons through optical fibres or free space; these moving quantum particles are often called 'flying qubits'. For the purposes of quantum communication, the end nodes and repeaters contain devices that can operate directly on the photons.

The end nodes typically perform quantum information processing on the transmitted data. This can be as simple as measurements of individual qubits, or as advanced as fully fledged quantum computation. Information processing will generally be implemented via whatever medium is most convenient. Currently, the leading technologies for quantum computing are superconducting qubits and ion traps, both of which encode the information in static particles that cannot move [Gibney, 2020]. This means that an efficient quantum device that can act as an interface between the static and flying qubits is necessary, sometimes known as a transducer [Caleffi et al., 2018]. Such interface technologies are also required for quantum repeaters and memories – equally important components in a quantum network as discussed directly below. Promising progress is being made to engineer such devices (see e.g. [Yang et al., 2016]) although these technologies are yet some way away from practical use.

3.5.2 Transmission methods and errors

The biggest hurdle in creating long-distance quantum communication networks is overcoming the errors in transmission, which scale exponentially with the length of the transmission line.

The best communication channel for photons on Earth is an optical fibre. When a photon travels through an optical fibre, there are two possible sources of error. Firstly, the photon can simply be absorbed in the fibre, leading to loss of the photon (e.g. as described by the erasure channel). Secondly, errors can occur in the polarisation state itself, for example a qubit initially encoded in the horizontal polarisation state $|H\rangle$ can be transformed into a random probabilistic mixture of horizontal and vertical polarisation states, $(1-q)\,|H\rangle\langle H| + q(|H\rangle\langle H| + |V\rangle\langle V|)/2$ (an example of a depolarising error). The probability of either of these errors occurring scales exponentially with the length of the transmission line L [Briegel et al., 1998]. This follows from the fact that the probability of error per unit length is constant, so the probability of no error decays exponentially with length.

With current technology and projected improvements of the same technologies, direct communication of single photons on Earth is limited to 500km due to loss. This is calculated from the assumption of a maximum photon generation rate of 10 GHz (10^9 photons per second), a minimum possible fibre optical loss of 0.15dB/km and a minimum required number of photons received at the other end of 100 photons per second [Gisin, 2015]. Further details on the experimental challenges are presented in §4.3.2.

An alternative way to transmit qubits between distant locations on Earth is via satellite communication. In this case, a photon is sent directly through free space to a satellite, which relays it back to another location on Earth. This has the advantage that there is less noise in

space than in the air close to the surface of the Earth or in terrestrial optical fibres. Recent experiments with the Micius satellite launched from China have demonstrated communication of independent single-photon qubits via quantum teleportation from ground level to the satellite at distances of up to 1400 km [Ren et al., 2017].

3.5.3 Long-distance transmission: quantum repeaters

One promising solution to the problem of scaling, as is done in classical communication networks, is to install intermediate nodes, called 'repeaters', between the sender and receiver. Classically, repeaters typically (a) amplify the signal, or, (b) detect and re-transmit. However, neither of these options are directly possible in the quantum case. (a) is prevented by the no-cloning theorem (an unknown quantum state cannot be copied) and (b) is prevented by the fact that measurements collapse the quantum state into one of the classical outcomes.

The paradigm of quantum repeaters all together discards the idea of sending the photon across the entire distance between the sender and receiver, and instead aims to distribute an entangled state between the two parties which would allow them to communicate quantum information using quantum teleportation [Gisin, 2015]. First, an entangled state is created between each pair of adjacent repeaters, between Alice and her closest repeater, and between Bob and his closest repeater. This only requires the transmission of one half of a fixed entangled state between two nearby nodes, which are positioned close enough so that transmission errors are tolerable. Now, consider any three adjacent repeaters A, B, C. It is possible to perform operations at each of the repeaters which convert the two entangled states between nodes $A - B$ and $B - C$, respectively, into a single entangled state between nodes $A - C$. This is known as entanglement swapping [Briegel et al., 1998]. Generalising over the whole network of repeaters in this way, it is possible to create entanglement between Alice and Bob at arbitrarily long distances apart, by only ever transmitting any physical quantum particle over a short distance with negligible errors.

A practical problem with quantum repeaters is that they require all the operations on the different entangled states to be synchronised in time. In particular, photons travel at the speed of light, so a photon localised at a repeater at a particular point in time cannot be easily be stored. This means that quantum repeaters are not possible without quantum memories – devices that allow a quantum state to be stored in a stationary quantum system, e.g. an atom, and then retrieved on demand.

3.5.4 Storage of quantum information: quantum memories

In a classical communication scenario, once the information sent by Alice has been received by Bob, Bob is able to freely store his information in a long-term computer memory, which can be freely accessed at a later time. This is done by copying the received information onto the memory system. For quantum information, however, the no cloning theorem prevents the possibility of copying the received information. Quantum memories address this problem by transferring, rather than copying, the information from the received qubits onto 'mem-

ory qubits'. Note, that by the no cloning theorem, once the state has been transferred from the photon to the memory system, then the photon itself must have changed state. (N.B. if only classical information is to be sent through the quantum channel, then detection and re-transmission would in principle be possible. However, usually the point of sending classical information through quantum channel is to enhance its transmission via quantum resources, such as shared entanglement, which would be destroyed in a measurement.)

The memory qubits are required to be stationary systems (e.g. atoms, ions, etc.), unlike photons which always move at the speed of light. They are also designed to be less susceptible to noise than the qubit systems used for the processing of the communicated information [Freer et al., 2017]. Recall, that in general, the state of a quantum system can only be maintained for a fraction of a second – the *coherence time* of the system (for atoms this can be of the order of milliseconds). This means that in the absence of additional procedures, the length of time quantum information can be stored is limited by the coherence time of the information-carrying system.

The successful implementation of a quantum memory requires several requirements to be met. First, the transfer of information from the received qubit onto the memory qubit must be fast and efficient enough to avoid significant losses of information. Secondly, the coherence time of the memory qubit must be long enough to store the information for the required amount of time. (Note, that this time will still be of the order of tens of milliseconds). Finally, the quantum memory must contain a fast and efficient protocol to transfer the information back onto a physical system suitable for information processing or further communication.

Typical coherence times of different systems vary greatly. Recent experiments have pushed the boundaries of coherence times for isolated systems; for an ensemble of nuclear spins a record of 6 hours was demonstrated in 2015 [Zhong et al., 2015] and for individual qubits (as required for quantum memories) a record of 1 hour was presented in 2021 [Wang et al., 2021]. However, for fully fledged quantum repeaters allowing the transfer of information from and to photons, the current limits are several orders of magnitude shorter. For example, in 2016 the lifetime of a quantum repeater with atom-photon coupling and memory stored in cold atoms was demonstrated up to 0.22 seconds [Yang et al., 2016] (an order of magnitude higher than than the previous record), which was calculated to be sufficient to perform entanglement distribution up to 1000 km. Note, however, than an experimental demonstration of such technologies in practice for communication still requires significant work in integrating the memories into working communications systems.

3.5.5 Key use-cases of the quantum internet

Here, three of the main future use-cases of the communication of quantum information across quantum networks are outlined, motivating the construction of a global quantum internet.

(a) **Distributed quantum computing.** The advent of quantum computing opens the potential to solve hard or resource-intensive computational problems, with applications ranging from cybersecurity to financial modelling and drug discovery. However, as in

the case of conventional computers, many computational problems require the combined effort of multiple interconnected processors, for example in distributed systems. Distributed quantum computing refers to connecting multiple small-scale quantum processors to form an effective larger, more powerful quantum computer. This will enable it to take advantage of superior resources and processing power by implementing quantum algorithms on distributed hardware to solve computational problems which may be intractable on individual quantum processors [Wehner et al., 2018].

(b) **Quantum cloud computing.** Quantum computers in the future are expected to perform a similar function to today's supercomputers, in the sense that typically only large institutions will have one on-site, whilst access to them is provided remotely via the cloud. Quantum cloud computing refers to forming a quantum cloud from a network of locally hosted processors, which can be accessed by distant users in a similar way to classical cloud computing [Caleffi et al., 2018].

(c) **Ultraprecise quantum clocks/GPS** refers to using precision meteorology with quantum networks to operate a network of distant atomic clocks across large geographic distances, at close to the fundamental physical limit of precision. This uses entangled quantum states and quantum communication between the clocks to enable the possibility of extremely precise clock synchronisation and GPS, which moreover has quantum-guaranteed security against both internal and external threats [Komar et al., 2014].

3.6 Communication with quantum control of transmission lines

As outlined in the introduction, it can be argued that the transition from classical to quantum is in a sense not fully captured by standard quantum Shannon theory, as the configuration of the transmission lines has so far still been assumed to be classical. However, as the iconic double slit experiments illustrates, quantum particles can also propagate in a superposition of trajectories. This has led to a variety of recent work on a generalisation to a second level of quantisation of Shannon theory, where both the information carrying-degrees of freedom and the configuration of the transmission lines can be in a quantum superposition [Ebler et al., 2018, Abbott et al., 2020, Chiribella and Kristjánsson, 2019].

The physical way in which this new paradigm is achieved is by using the trajectory of the particle as a quantum control system, whilst information is encoded in an internal degree of freedom of the particle [Chiribella and Kristjánsson, 2019]. For the standard example of using single photons, this means that the spatial mode of the photon acts as a quantum control, whilst the information is encoded in e.g. the polarisation of the photon.

In addition to this paradigm of quantum Shannon theory with superpositions of trajectories, several other paradigms within the second level of quantisation of Shannon theory have been proposed, where other elements of the configuration of transmission lines can be in a quantum superposition. For example, the time of transmission, the order of the transmission lines, or

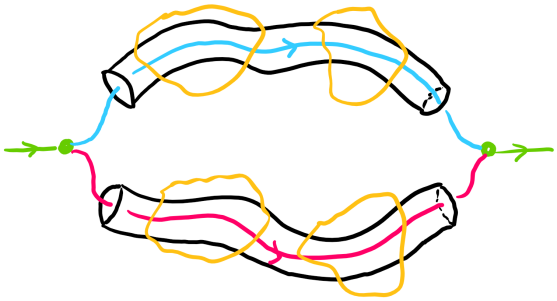

Figure 8: A single particle sent through two transmission lines in a superposition of two different trajectories (blue and magenta, respectively). On each trajectory, the particle experiences different errors (yellow regions).

even the direction of communication – enabling the possibility of two-way communication with only a single particle. [Del Santo and Dakić, 2018]. In the following sections, the extended paradigm of quantum Shannon theory with superpositions of trajectories is explored in detail, followed by the superposition of the direction of communication. The extended paradigms of quantum Shannon theory with superpositions of the time of transmission and quantum Shannon theory with superpositions of the order of transmission lines are described in a similar way and are thus left to Appendix C. For each of these new paradigms, examples of their advantage in communication over standard quantum Shannon theory are presented.

3.6.1 Quantum control over trajectories

Consider a standard communication scenario from Alice to Bob. Alice prepares a photon, encoding information in its polarisation state, and sends it to Bob through an optical fibre (mathematically described by a quantum channel). Any given optical fibre will subject the photon to noise, with fixed probability of error. Now, with access to two separate optical fibres, Alice could initialise her photon in a quantum superposition of travelling through one optical fibre or the other. Strikingly, sending a single particle in a superposition of two noisy transmission lines can result in an effective transmission line which is less noisy than either of the original ones individually [Gisin et al., 2005].

Mathematically, we describe the situation as follows: The polarisation of the photon, which is used to encode the message, is described by a quantum state

$$|\psi\rangle = \alpha\,|H\rangle + \beta\,|V\rangle\,, \tag{72}$$

where $|H\rangle$ and $|V\rangle$ are the basis vectors of horizontal and vertical polarisation, respectively, and α, β are complex numbers. Alice is able to prapare any such state of her choice, as described in §3.1.

Now, the path taken by the particle is also described by a quantum state of its spatial mode, this time fixed in an equal superposition of the states $|L\rangle$ and $|R\rangle$, corresponding to the particle travelling through the left-hand transmission line or the right-hand transmission

line, respectively:

$$|+\rangle = \frac{1}{\sqrt{2}}(|L\rangle + |R\rangle). \tag{73}$$

Overall, the full quantum state of the photon is described by the composite state

$$|\psi\rangle_M \otimes |+\rangle_P , \tag{74}$$

where we use the subscripts M and P to denote message and path, respectively.

So far, the situation is analogous to the double slit experiment, where additionally the photons have information encoded in their polarisation (recall, that the double slit experiment was not about information – only the spatial mode was used, which was initialised in an equal superposition of two separate paths). From now, the novelty of this paradigm will become apparent: not only does the particle propagate in a superposition of two paths, but on each path different transmission lines act on its polarisation degree of freedom, adding independent noise to the message on each of the two paths. This creates entanglement between the message and path degrees of freedom, which is key to the communication advantages observed.

Consider a general noisy channel $\mathcal{N}$ from Alice to Bob, for example an optical fibre. When Alice sends her photon initialised in the state $\rho = |\psi\rangle\langle\psi|$ through this channel only, then the state received by Bob will be given by $\mathcal{N}(|\psi\rangle\langle\psi|)$. (For example, in the case of a completely depolarising channel, which simply converts the state into white noise, $\mathcal{N}(|\psi\rangle\langle\psi|) = I/2$.) However, if Alice sends a particle in a superposition through two identical optical fibres, each described by the channel $\mathcal{N}$, then the state received by Bob is given by

$$\mathcal{S}(\rho \otimes |+\rangle\langle+|) = \frac{\mathcal{N}(\rho) + F\rho F^\dagger}{2}_M \otimes |+\rangle\langle+|_P + \frac{\mathcal{N}(\rho) - F\rho F^\dagger}{2}_M \otimes |-\rangle\langle-|_P , \tag{75}$$

where F is an operator which depends on the specific way in which the communication device behaves when no state is transmitted through it (in physics terms, the vacuum state is transmitted) [Chiribella and Kristjánsson, 2019]. In general, the terms $F\rho F^\dagger$ depend on the input state ρ, meaning that the terms

$$\frac{\mathcal{N}(\rho) \pm F\rho F^\dagger}{2}_M \tag{76}$$

also depend on ρ even if $\mathcal{N}(\rho)$ is very noisy. This means that Bob can perform a measurement on the path qubit P in the $\{|+\rangle / |-\rangle\}$ basis, and then perform an appropriate decoding operation on the message qubit M to retrieve (with potentially less noise) the information sent by Alice.

Physically, what has happened here is *destructive interference* between the noise happening on the left-hand transmission line and the noise happening on the right-hand transmission line. This is analogous to the destructive interference of ripples in water; when two ripples

from opposite directions coincide, they will cancel each other out in specific locations.

For different types of noise, the superposition of paths can yield different sorts of advantages. To illustrate these advantages, we consider two extreme cases, where (a) two completely depolarising channels (which individually have zero classical capacity) are converted into an effective transmission line with non-zero classical capacity, and (b) two completely dephasing channels (which individually have zero quantum capacity) are converted into an effective transmission line with non-zero quantum capacity.

First, consider the scenario where Alice has access to two optical fibres that each act as a completely depolarising channel

$$\mathcal{N}_{\text{dep}}^{p=1}(\rho) = \frac{I}{2} \tag{77}$$

on her polarisation qubit. This has zero classical capacity, and no matter how many times she sends a single photon in a definite path through one of these two channels, Bob will not be able to receive any information. However, using Equation (75), it can be seen that sending the photon through the two completely depolarising channels in a superposition of paths yields an output state with a non-trivial dependence on ρ. Using the qualifications of capacities presented in Appendix B, the Holevo information (a lower bound to the classical capacity) of a single completely depolarising channels is zero, whilst *between 0.05 and 0.16 bits per channel use* when two such channels are used in a superposition of trajectories (depending the specific implementation as specified by the operator F) [Abbott et al., 2020, Kristjánsson et al., 2020]. Since the Holevo information is a lower bound to the classical capacity, this protocol achieves the possibility of non-zero classical capacity through two zero-capacity channels – an infinitely large increase in the classical capacity by using the channels in a quantum, as opposed to a classical, configuration.

Secondly, consider a scenario where Alice has access to two optical fibres that each act as a completely the dephasing channel

$$\mathcal{N}_{\text{deph}}^{p=1}(\rho) = \langle 0|\,\rho\,|0\rangle\,|0\rangle\langle 0| + \langle 1|\,\rho\,|1\rangle\,|1\rangle\langle 1|\,. \tag{78}$$

on her polarisation qubit. This has zero quantum capacity, meaning that however many times she sends a single photon in a definite path through one of these two channels, no quantum information can be transmitted to Bob. Yet, by using two such channels in a superposition of paths, the output received by Bob (assuming a specific F [Chiribella and Kristjánsson, 2019]) will be given by

$$\mathcal{S}(\rho \otimes |+\rangle\langle +|) = \frac{Z\rho Z}{2}_{M} \otimes |+\rangle\langle +|_{P} + \frac{2\rho + Z\rho Z}{2}_{M} \otimes |-\rangle\langle -|_{P}\ , \tag{79}$$

where $Z = |0\rangle\langle 0| + |1\rangle\langle 1|$ is the (unitary) Pauli-Z matrix. Recall, that unitary operators are completely correctable, in this case $Z^2 = I$. Thus, we see that Bob can measure the path qubit P in the $\{|+\rangle\,/\,|-\rangle\}$ basis, and conditionally upon a $|+\rangle$ result (which occurs with 25% probability), the polarisation qubit collapses to the state $Z\rho Z$, which Bob can correct by simply

applying his own Z operation, to recover the original state ρ. Thus, whenever Bob obtains the $|+\rangle$ outcome (this occurs in 1 out of 4 runs of the protocol), we obtain an effective transmission line with perfect quantum capacity of *1 qubit per channel use* [Chiribella and Kristjánsson, 2019]. This means that by using these transmission lines in a quantum configuration, we achieve an increase from 0 to 1 in the quantum capacity – an infinitely large improvement – compared to using the transmission lines in a classical configuration.

Recall, that these results, as in the rest of this chapter, pertain only to the capacities of quantum channels themselves – physically corresponding to (simplified models of) transmission lines. The creation and detection of information-carrying photons also have their own sources of noise, which are discussed in §4.

These theoretical predictions and other similar ones have been experimentally verified in recent works [Lamoureux et al., 2005, Rubino et al., 2021] and further experimental proofs of principle investigating these effects in more detail are currently underway at the Department of Physics, Imperial College London.

3.6.2 Quantum control over the direction of communication

In ordinary communication protocols, be it classical or quantum, either Alice sends information to Bob, or Bob sends information to Alice. Of course, if they each have access to their own particle, then Alice could send her particle to Bob at the same time as Bob sends his particle to Alice, achieving simultaneous two-way communication. Yet, a recent work has showed that quantum theory enables two-way (classical) communication using only a *single* quantum particle [Del Santo and Dakić, 2018].

This is done by initialising the particle in a superposition of two locations, at Alice (A) and at Bob (B). In physics terms, when the particle is absent at a give location, the 'vacuum' is present in that location. In equations, we write

$$|\psi\rangle = \frac{|\text{particle}\rangle_A \otimes |\text{vacuum}\rangle_B + |\text{vacuum}\rangle_A \otimes |\text{particle}\rangle_B}{\sqrt{2}} \tag{80}$$

Alice and Bob are both able to perform operations on their 'half' of the particle (which physically, corresponds to some operation on either the particle or on the vacuum, or a coherent superposition of the two). To send one bit each of classical information, they can each encode their desired bit in the phase their 'half' of the particle, (this is a unitary operation, so allowed). We call Alice's and Bob's bit values a and b, respectively, each of which can take value either 0 or 1. Then the resulting state is:

$$|\psi\rangle_{ab} = \frac{(-1)^a |\text{particle}\rangle_A \otimes |\text{vacuum}\rangle_B + |\text{vacuum}\rangle_A \otimes (-1)^b |\text{particle}\rangle_B}{\sqrt{2}} \tag{81}$$

After the encoding, Both parties send their state through a beamsplitter V, a device which partially reflects back and partially transmits to the other other party. It can then be shown that whenever Alice and Bob send the same bit value, the particle ends up deterministically at Alice,

and whenever Alice and Bob send a different bit value, the particle ends up deterministically at Bob. That is,

$$V\left|\psi\right\rangle_{a=b} = \left|\text{particle}\right\rangle_A \otimes \left|\text{vacuum}\right\rangle_B \tag{82}$$

$$V\left|\psi\right\rangle_{a\neq b} = \left|\text{vacuum}\right\rangle_A \otimes \left|\text{particle}\right\rangle_B . \tag{83}$$

This means that they can both perform a measurement to check whether or not they have received the particle at the end. Depending on who has the particle, both parties can thus determine the bit value sent by the other. This protocol has recently been experimentally demonstrated in [Massa et al., 2019].

3.6.3 Discussion

We have seen that the use of quantum communication channels in a quantum configuration (of trajectories, times, or orders) enables the possibility of an enhancement of the classical and quantum capacity of the channels.

An important point to note here is that these comparisons of communication enhancements need to be restricted to scenarios in which the quantum states of the trajectories, times or orders do not themselves act as information carriers, i.e. Alice cannot access the states of the configurations. Otherwise, the paradigm simply reduces to standard quantum Shannon theory with a larger space of possible information carriers [Chiribella and Kristjánsson, 2019, Kristjánsson et al., 2020]. Of course, directly using the spatial modes of photons to encode information is itself also an established paradigm (albeit useful in different situations to the polarisation encodings focussed on here), as introduced above. The combination of scenarios in which the spatial modes are used both as a quantum control of other degrees of freedom (e.g. polarisation) and to directly encode information can be expected to yield further interesting protocols for quantum communication, see e.g. [Guérin et al., 2019].

The second level of quantisation of Shannon theory has proven that elevating the configuration of transmission lines to a quantum degree of freedom yields new possibilities for communication, even when the configuration degrees of freedom are not directly used to encode information. In a similar spirit, we have seen that a single particle can enable perfect communication between two parties, even if each party only sends and receives the particle once.

4 The technical challenges of implementing quantum communication in practice

Following the theoretical description of extensions of Shannon theory to the quantum regime, this section will deal directly with the physical implementation of the architecture required for genuine quantum information transfer and communication networks.

A review of photons and quantum optical fields is covered as well as various choices of encoding schemes, including their feasibility and challenges. Key components of a quantum optical system, which both standard quantum communication and its extensions to a second level of quantisation rely on, are also outlined. In particular, photon generation, quantum information transmission and photon detection – all of which play important parts in the theory reviewed in the previous section – are discussed.

4.1 Optical bits

Optical fields are already a key component of classical information transfer systems. The advent of optical fibre communications has yielded dramatic improvements on data bandwidths, and allowed information to travel at close to the speed of light. Compared to copper cable type communications, the reliability and range of transmission has developed significantly, owing to the technological advances in the development of low–loss and low–noise optical fibres.

A new paradigm for further advances exists in the quantum regime, moving from optical fields to photons. While an abstract take on shifts beyond classical Shannon theory has been outlined, there are significant hurdles to overcome before such schemes can be physically implemented beyond simple prototypes. The quantum features of light play a key role in this regard.

4.2 Photons as qubits

In addition to the advantages derived from the classical features of light – namely their low loss in optical fibres and fast transmission times – photons are also ideal carriers of quantum information [Flamini et al., 2018]. The key reason for this is that photons do not have strong interactions with their environment, and so errors in their quantum information are typically low compared to alternative physical platforms. As an example, photon polarisation states can be maintained in optical fibres across the order of 100 km, while stabilising neutral atoms in superposition states can only be achieved for milliseconds (and it would not be possible to transfer their quantum information across any appreciable distance in this time).

A key advantage of photonic implementations of quantum information is direct control over coherence time. As mentioned in section 2.2.2, coherence is important for qubits to interfere and interact with one another – this is especially important for performing quantum algorithms. The idea of photon coherence follows from a classical notion; photons can be described as wavepackets with a spectral spread (known as a photon's bandwidth), which is

the Fourier transform of the wavepacket's temporal description (i.e. the length of the photon). This is distinct from data bandwidths, and, rather than indicating the rate of information transfer, it is an important parameter for considering photon–matter interactions e.g. for quantum memories (see later). Different spectral components of the wavepacket pick up phases at different rates – eventually the wavepacket will not be coherent because it's spectral components are not in phase with one another. This would remove interference phenomena (e.g. the resulting quantum interference pattern from the double slit experiment), and remove quantum effects. Photonic implementations of quantum information offer control over the photon's bandwidth (different generation mechanisms yield varying widths), which in turn gives control over the coherence time of a photon. As an example, single photons generated from trapped ions have wavelengths close to 750 nm and spectral bandwidths close to 10 femtometres, which gives coherence times of 60 ns and corresponding coherence lengths of up to 20 m (suitable for table-top interference experiments to implement photonic quantum algorithms). State of the art photonic coherence times have exceeded 1μs, yielding coherence lengths of over 300 m [Zhao et al., 2014]. While in the classical case, coherence typically refers to the spectral distribution of light, for quantum interference a range of degrees of freedom (in addition to frequency spectrum) need to be considered, although these are typically not limiting factors e.g. polarisation states can be maintained for hundreds of kilometres. In addition to a photon's temporal / spectral description, these degrees of freedom include photon polarisation and a photon's (internal) spatial mode (see encoding schemes for a fuller account).

Coherence for most quantum systems typically require cryogenic temperatures. For example, in trapped ions, heating causes an ion to vibrate accumulating random phases which destroy any prospect of quantum interference required for the implementation of quantum protocols. This is not the case for the photonic platform – coherence is maintained at room temperature because photons do not interact strongly with their environment. This offers a major advantage in terms of feasibility and cost.

Photons could also act as carriers of quantum information between different physical platforms [Meyer et al., 2015]. For example, there is ongoing work in atom–light coupling and ion–light coupling, and photons could potentially map quantum information from one system to another. This is especially useful in systems where scaling is an issue; photons could act as information carriers between small modules, which could offer a feasible route to scaling quantum architectures, culminating in the possibility of distributed quantum computing (see §3.5). In this sense, photons as information carriers will be a central player in future quantum technologies, independent of the development of alternative platforms – their robustness against decoherence at room temperature and ability to transmit information quickly across large distances gives them an unparalleled advantage.

Quantum information and communication systems have already been demonstrated, albeit on a small scale, with photonic qubits. Free space entanglement-based quantum key distribution has been demonstrated over distances of 7500km and allowed for genuinely quantum secure information transfer through the use of satellites [Dequal et al., 2016]. Limitations still exist however; information transfer rates are low and environmental conditions (explored

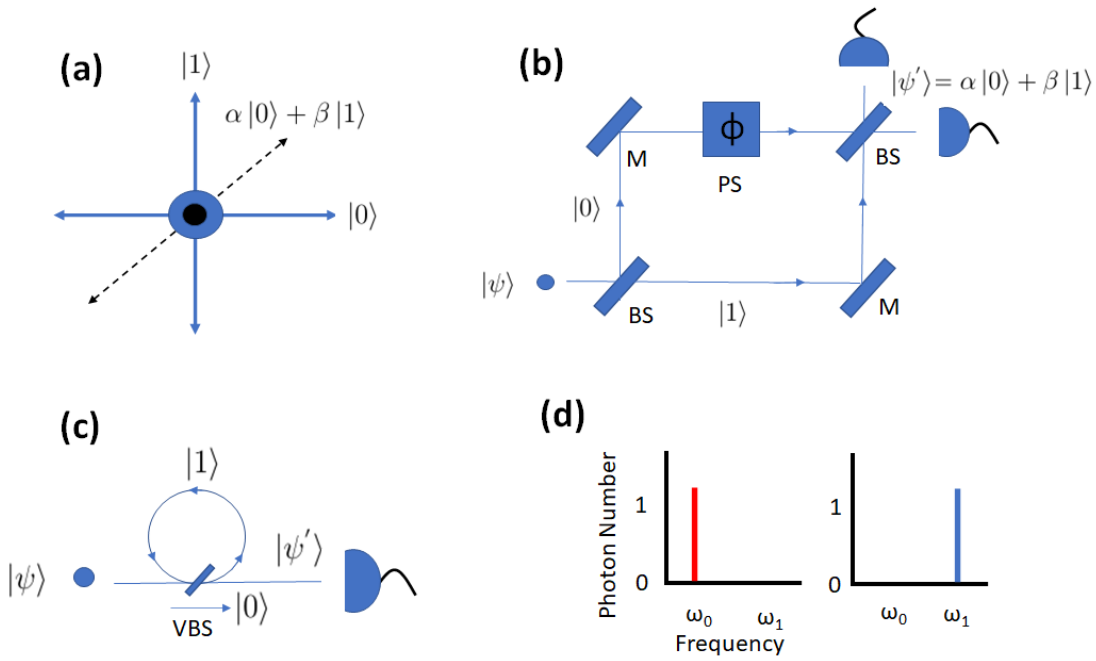

Figure 9: Different photonic encoding schemes for quantum systems. (a) Polarisation encoding; the classical pure states are the horizontal ($|0\rangle$) and vertical ($|1\rangle$) polarisations, while diagonal, circular and elliptal states represent superpositions. (b) Mach–Zehnder interferometer commonly used for spatially encoded qubits. A photon enters through a beamsplitter, reflecting off a series of mirrors, with one path undergoing a controlled phase shift to control the output superposition of the photon. (c) Time-bin encoded qubits in a loop structure. A photon's superposition can be controlled using a variable beamsplitter to determine the degree to which the photon enters the loop. (d) Frequency encoded qubits, with different monochromatic frequencies representing $|0\rangle$ and $|1\rangle$.

in 4.3.2) have significant impacts on the use of the quantum channel.

More recently, building upon classical fibre networks, quantum teleportation using time-bin encoded qubits was demonstrated across 44km [Valivarthi et al., 2020]. These demonstrations are key checkpoints on the journey towards a genuinely quantum internet.

Another significant milestone in photonic quantum information was the demonstration of quantum computational advantage, performing an algorithm which is impossible (exponentially hard) with classical systems [Zhong et al., 2020]. Further advances on this experiment are at the forefront of research, signifying a new regime in which photonic qubits will offer quantum advantage over classical systems.

4.2.1 Encoding schemes

Photonic qubits can be encoded in various ways, by taking advantage of the various degrees of freedom available to photons; and the options are outlined in this section. As has been the main theme in this report, encoding choice is motivated by two key areas,

1. Suitability for quantum communication; effects on data bandwidth, capacity, security and ease of transfer. The focus here is on the transfer of *quantum information*, as opposed to classical information.

2. Suitability for performing useful quantum protocols. Important factors here involve ease of photon interference and entanglement, scalability and coherence times.

Many options are possible in the photonic regime – in the previous chapter, it was seen that (pure) qubit states can be written as,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{84}$$

and that photonic qubits are often encoded in the two orthogonal polarisations of a single photon (see figure 9a). The state vectors for these qubits are commonly notated as $|0\rangle \rightarrow |H\rangle$ for the horizontal state and $|1\rangle \rightarrow |V\rangle$ for the vertical state. Polarisation states remain stable over long distances (currently quantum communication using polarisation entangled photons has been demonstrated across 100 km lengths of optical fibre) and they are relatively easy to manipulate using readily available components in both free–space and fibre–based settings, which is why they are a common encoding choice. As mentioned in section 2.1, polarisation encoded photons have a close link to classical systems. Their description via the Bloch Ball is directly analogous to the Poincaré Sphere. The 'classical' pure states on the z-axis are the vertical and horizontal polarisation states, the x-axis describes linear mixtures of these, yielding diagonal and anti–diagonal polarisations, while the y-axis, which introduces an imaginary component, gives rise to circularly polarised states. Elliptically polarised states lie elsewhere on the surface of the Bloch Ball. The case of horizontal, vertical and linear mixtures of them (i.e. diagonal and anti-diagonal polarisations) is represented graphically in figure 9a ; circular and elliptical polarisations include additional phases which are not represented.

However, photons have many degrees of freedom and other forms of encoding are possible which offer distinct advantages [Slussarenko and Pryde, 2019].

Another common approach is to use spatially encoded photonic qubits – this was seen previously in the example of a travelling photon. On table top experiments, separate paths that a photon can travel down represent different classical pure states, e.g. for the case of two distinct paths, one path represents $|0\rangle$, while the other represents $|1\rangle$. Photons can be sent down a superposition of the two paths, which is represented by positions off the z-axis on the Bloch Ball. Spatially encoded qubits are typically manipulated using beam–splitters, which control the degree to which a photon travels down a particular path, and mirrors, which direct photons along a given path. Pure state, single qubit manipulations (i.e. moving a qubit's Bloch vector around the Bloch Ball) are commonly performed using Mach–Zehnder interferometers (see figure 9b) in a regime known as 'dual rail' encoding. A photon from one arm (in state $|0\rangle$) enters the interferomter via an initial 50:50 beam splitter, which evolves the photon into the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. One path contains a controllable phase–shift, often implemented experimentally via an external voltage or temperature control. The photon exits the inter-

ferometer via another beam splitter, and measurements using single–photon detectors on each exit arm can be performed. The detector that measures the photon will indicate which path the photon's quantum state has collapsed to. The phase shift and final beam splitter allows for single qubit rotations around the Bloch Ball; it gives control over the coefficients (α and β) of the output state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. This single qubit example generalises when the number of spatial paths in the system increases – e.g. for four paths (labelled by $|0\rangle, |1\rangle, |2\rangle, |3\rangle$), two qubits could be encoded in the following way $|0\rangle = |00\rangle$, $|1\rangle = |01\rangle$, $|2\rangle = |10\rangle$, $|3\rangle = |11\rangle$. In general a system with 2^n paths can encode n qubits; unfortunately this results in exponential scaling of the number of paths required for a given number of qubits. This is clearly problematic for performing useful quantum protocols, because the number of paths required scales exponentially with the number of qubits. Similar transformations are possible in optical fibres; as an example, beam splitters are implemented by coupling evanescent fields of single photons to neighbouring fibres (brought in close proximity to one another).

It is clear that this encoding does not directly use an 'internal' degree of freedom of the photon itself, and in fact, it is known that $N \times N$ unitary gates can be performed with this encoding scheme using N^2 optical elements [Reck et al., 1994]. However this is resource inefficient and often impractical for large systems, requiring photon detectors on every spatial mode. Alternatives to this scheme have been suggested, which scale efficiently, but require highly non–linear interactions and result in probabilistic gate implementation [Knill et al., 2001].

While problematic for use in the implementation of quantum protocols and logic manipulation, spatially encoded qubits are a natural choice for communication systems. Alternatively, as seen in §3.6.1, the extended paradigm of quantum Shannon theory with superpositions of trajectories employs the spatial degree of freedom as a quantum control system of the photon, while the information itself is encoded in the photon's internal degrees of freedom (e.g. polarisation).

Time-bin photonic qubits are an alternative [Tan and Rohde, 2019]. These take advantage of the speed of light, and define different qubit basis states and detections at separate points in time – in the qubit case, only two time bins are needed. A common set–up is shown in figure 9c, whereby photons can be manipulated to travel through or past a loop of fibre (or in a superposition of both), through the use of a variable beam splitter. A variable beam splitter has reflectivity and transmissivity which can be varied, and is often controlled via an external voltage control – a Mach-Zehnder interferometer set-up can be used as an alternative and performs the same function. This loop structure is also scalable – trains of photons can enter the loop and interfere with one another at the beam splitter, via the so–called Hong Ou Mandel effect, after travelling different numbers of round–trips through the loop. So long as the variable beam splitter can be adjusted on the timescale of the photon train frequency, a similar architecture can be used to enact a universal set of unitary quantum gates. While the number of detectors and components is scalable, the corresponding draw–back is that quantum operations take time – roughly on the order it takes for a train of photons to travel

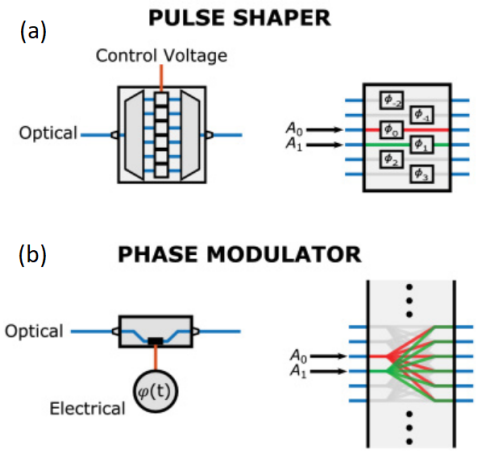

Figure 10: (a) A pulse shaper applies arbitrary phases to each spectral mode. In practise this is implemented by separating and recombining frequency modes (left), and can be thought of as applying mode-specific phase shifts (right). (b) Electro-optic modulators cause temporal phase shifts (left). This can be thought of as a mode mixer that can change a photon's frequency mode (right). A_0 and A_1 are example input qubits of different frequencies, representing $|0\rangle$ and $|1\rangle$. Figure adapted from [Lukens and Lougovski, 2017].

through the loop architecture. At present, variable beam splitters in this architecture can be adjusted at MHz speeds – this will need to improve by several orders of magnitude (i.e. GHz/THz) to allow time-bin qubits to be a viable encoding system for useful quantum protocols.

While gates for interacting time–bin encoded qubits in the near term in a quantum communication system is unlikely, the use of the encoding scheme for the communication of quantum information could be viable. In this instance, photons would be sent down a superposition of paths of different lengths, and the state of a qubit would be registered by the time it hits a photon detector rather than (as in the spatially encoded case) hitting a detector on a particular path. A key limitation here is the rate at which detectors can perform a series of consecutive measurements; a train of photons cannot be separated by times less than this, otherwise some photons will not have a chance of being detected (see section 4.3.3 for more details). Importantly, the Holevo bound (§2.2.6) limits the capacity of single qubits – they can offer no more than a single bit of classical information – although, as mentioned in §3.2.2, the use of entangled quantum states (i.e. multiple qubits with quantum correlations) may offer methods to move beyond classical limits.

Photonic qubits can also be encoded spectrally [Lukens and Lougovski, 2017]. For instance, in a simple model, two well–spaced monochromatic modes could act as a basis with $|0\rangle = |\omega_0\rangle$ and $|1\rangle = |\omega_1\rangle$ as the qubit states (shown in figure 9d). From the motivation of quantum protocols – which require photon interactions – necessary evolutions of spectrally encoded photons can be achieved via a combination of pulse shapers and electro-optical modulators. Pulse shapers cause a spectrally dependent phase delay, while electro-optical modulators, which give control of a photon's temporal phase, are able to mix photon modes of different frequencies – this is shown diagramatically in figure 10. By combining a series of these in-

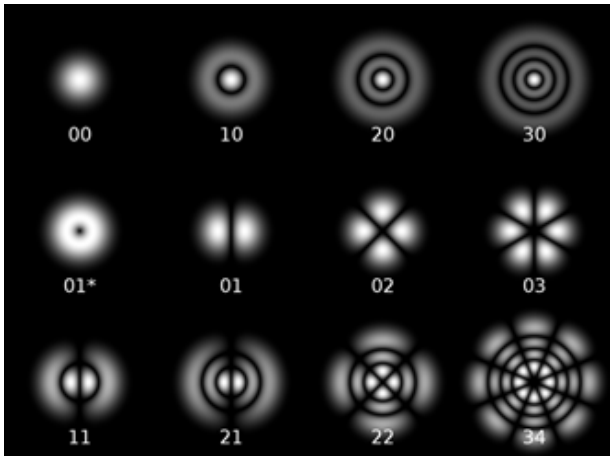

Figure 11: Different order spatial modes (labelled with two numbers) of light, including the fundamental Gaussian mode (00) and higher order Hermite–Gauss modes which act as orthogonal quantum information states $\{|0\rangle \ldots |d-1\rangle\}$.

struments (this can be technically challenging, and is an area of ongoing research), arbitrary unitary gates can be performed on a qubit to implement quantum protocols.

With regards to quantum communication, frequency encoded photons offer an exciting possibility because the spectral states are orthogonal. With appropriate filters and detectors, photons of different frequency can be treated independently from one another and so a single multimode fibre could transfer many photons in parallel, offering a linear increase in channel bandwidth proportional to the number of frequencies used. Dispersion may be an issue here, and certain processes (e.g. the implementation of quantum protocols) can cause photon frequency shifts. This will therefore require an appropriate spectral distance between different modes; placing a limit on the total channel bandwidth available.

While external spatial encoding has been described above, it is also possible to take advantage of a photon's internal spatial degrees of freedom [Erhard et al., 2018]. As well as existing in a range of possible frequency modes, photons are also described by a set of orthogonal spatial modes, typically a pure Gaussian mode with zero angular momentum (usually $|0\rangle$), and either Hermite-Gauss or Laguerre–Gauss for modes with non–zero angular momentum ($|1\rangle, |2\rangle \ldots$). While the $\{|0\rangle, |1\rangle\}$ subspace can be used for qubit systems, typically higher dimensional quantum information is encoded in order to take advantage of the many angular momentum modes available. Multi–qubit gates and algorithms for quantum protocols are still in early stage developments for this form of encoding, requiring coherent interactions between photons in different spatial modes – this is difficult to implement with current technology.

However, this form of encoding naturally lends itself to both free space transmission as well as transmission through multi–mode optical fibres. Because the angular momentum states are orthogonal, a multimode fibre has the ability to transfer higher dimensional quantum information, limited only by the control over a single photon's angular momentum state. For instance, a photon in a superposition of its first d angular momentum states $\{|0\rangle \ldots |d-1\rangle\}$ can offer the ability to transfer $\log_2(d)$ bits per photon, as set by the Holevo bound. The

initial generation of highly entangled quantum information is well developed in this encoding scheme. This could be used as an additional resource to increase communication capacities (with the caveat that entanglement is required). Also of interest is the fact that using higher dimensional quantum information increases a communication system's robustness to attacks from approximate cloning (true copying of quantum states is impossible due to the no–cloning theorem). This offers significant advantages for near–term uses in protocols such as quantum key distribution.

4.3 Communication systems

The basic structure of quantum communication systems has been outlined previously in the report. Here, the potential physical implementation of such systems is considered, broken down into three key areas: quantum state generation, transmission, and finally state detection. The specific details of various gate implementations are not outlined here, because it depends on the encoding scheme, although this has already been touched upon in the previous section.

4.3.1 Quantum state generation

The focus here is on single photon generation, which is typically used in discrete–encoding systems, although the generation of squeezed states of light is briefly mentioned.

Ideal single photons are characterised by a set of parameters that need to be optimised in order to improve the efficiency of the quantum communication system [Eisaman et al., 2011, Lounis and Orrit, 2005]:

- Wavelength and tunability: ideally the wavelength of the photon would be optimised for the communication system. Many applications match photons to the infrared C band (1530-1565nm wavelength) because fibre systems in this regime have extremely low levels of loss, which is a key obstacle in single photon transmission (see figure 12). Free space systems employ a range of alternatives including long wavelengths (4μm) and visible wavelengths for ease of use (0.65μm) [Gariano et al., 2017]. In the event that generated photons have different wavelengths, it is important to be able to correct this, typically up to nm step precision in order to control the distinguishability of different photons. This will give control over interactions between photons in the communication system.
- Photon bandwidth: all single photons can be described as a wavepacket travelling through space with a characteristic width in time. The Fourier transform of this gives a frequency profile, whose width is the photon's bandwidth. Control over the bandwidth is important – this parameter is crucial for interfaces between optical and atomic systems (e.g. in memories), where bandwidths of e.g. 1GHz are required [Michelberger et al., 2015]
- Photon internal spatial mode: this idea was introduced briefly through angular momentum encoding systems. This is similar to classical systems in the sense that single

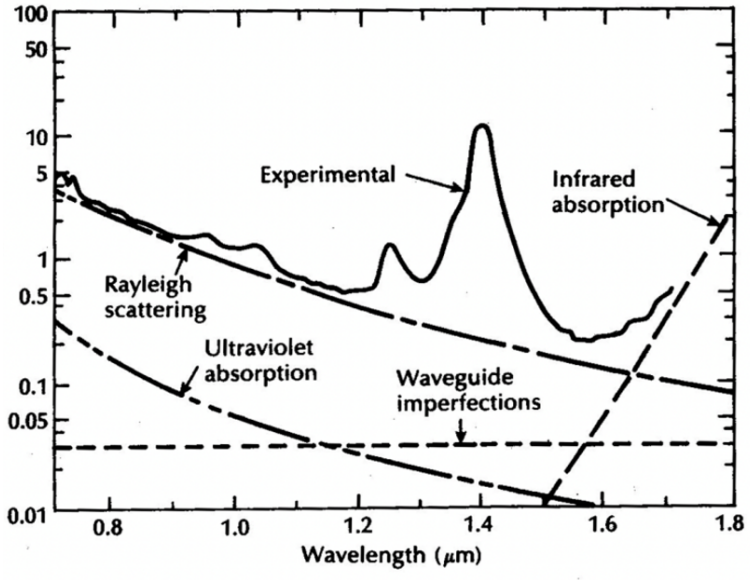

Figure 12: Loss (in dB) against wavelength for a given length of silica optical fibre. Low loss levels occur in the infrared C band, and so single photons are often matched to this wavelength. Various mechanisms for loss, such as Rayleigh scattering, ultraviolet absorption, waveguide imperfections and infrared absorption, which are identical in the classical and quantum cases are shown to describe experimental data.

mode fibres will only support Gaussian modes, while multi–mode fibres can support higher order modes. In the photon picture, the same principle applies, with the Gaussian mode corresponding to a photon with zero angular momentum, and higher order modes having non–zero angular momentum. Multimode systems could allow for higher communication capacities (as outlined earlier), while single mode light can increase photon-photon interactions required for quantum algorithms.

- Generation type: different mechanisms for photon generation are either inherently *probabilistic* or *deterministic*. In the probabilistic case, the probability of generation should be maximised, or, multiple generation sites used (known as multiplexing) in order to compensate.
- Generation temperature: a range of different temperatures are required for various forms of photon generation. In some instances, cryogenic temperatures are required for photon generation, for instance, photons generated from trapped ions. This creates additional costs for a quantum communication system.

One of the key areas that this report investigates is the transfer and subsequent manipulation quantum information. In the long term, it will be important to perform useful quantum algorithms using this information. To perform algorithms of interest, photons will be required to interact with one another, which typically requires them to be indistinguishable. In addition, these photons require high purity, which means that they should be close to being a quantum pure state, on the surface of the Bloch Ball (§2.1.3) (rather than a mixture of states).

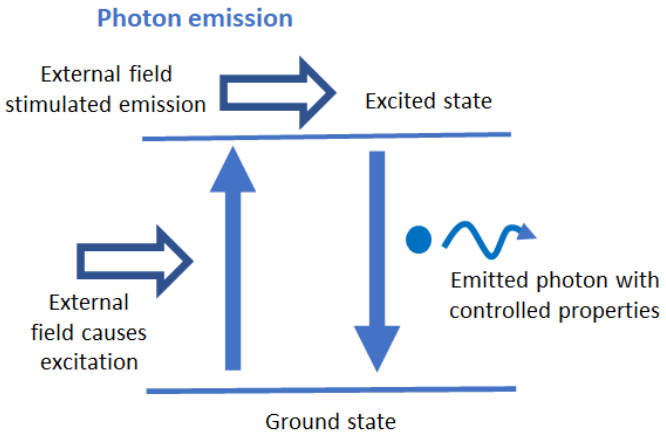

Figure 13: Basic diagram of photon emission. An external field causes both excitation of, and subsequent stimulated emission of, a photon with controlled properties.

There are a variety of different physical methods for generating single photon states. Common choices are briefly outlined below, with a focus on their ease of implementation as well as the challenges they pose.

Single atoms have a set of discrete energy levels which can be exploited to emit single photons [Buller and Collins, 2009]. In general, the interaction can be thought of as an external field interacting with two levels, a lower energy 'ground state' level $|g\rangle$ and a higher energy 'excited state' level $|e\rangle$. The atom begins in the ground state and is excited to the excited state by an external light field (laser). The atom undergoes stimulated emission, decaying back to the ground state, releasing a photon in the process (shown in figure 13). In reality the details are somewhat more involved, typically involving two separate ground states. Single neutral atoms, can be stored and cooled in a magneto–optical trap, and subsequently dropped through a cavity (two opposing reflectors). As the atom passes through the cavity, an external field excites the atom from state $|g^{'}\rangle \rightarrow |e\rangle$, and, because the cavity is correctly engineered, a subsequent decay takes the atom from $|e\rangle \rightarrow |g\rangle$, which is an alternative ground state. This process can be performed coherently and is known as *stimulated Raman adiabatic passage* (STIRAP [Vitanov et al., 2017]). The three level system is needed so that the energy of the emitted photon is distinguishable from the applied external field. This approach generally yields high efficiency of generation, although losses and fluctuations in the cavity can be high and generation is limited by the atom's time spent dropping through the cavity [Higginbottom et al., 2016].

A similar implementation to STIRAP (e.g. far detuned Raman processes) can be applied to single ions (charged atoms) [Barros et al., 2009]. In this instance, ions can be held in precise positions (nm scale) by electric and/or magnetic fields, and an external field can be applied directly, giving high emission rates. The energy levels involved are generally ultraviolet transitions, leading to competition between desirable stimulated emission, and unwanted spontaneous emission which yields photons with less well-controlled properties. In addition, ion systems

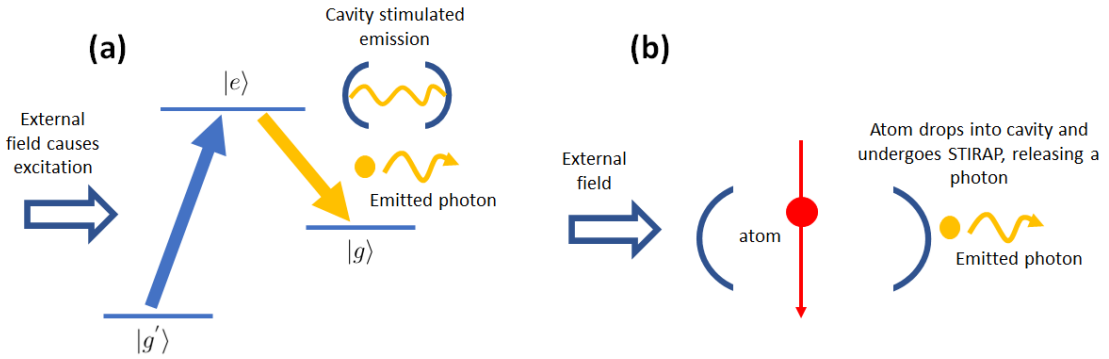

Figure 14: STIRAP procedure. An external field excites an atom which subsequently drops into a cavity (between to mirrors). The cavity causes stimulated emission of a photon and the atom moves to an alternative ground state. This allows the emitted photon to be distinguishable from the applied external field.

suffer from similar loss problems to neutral atom systems.

A promising route to single photon generation is through 'quantum dots' [Arakawa and Holmes, 2020]. These systems are grown from semiconductor material, and the confinement of quantum dots over small spaces creates a discrete energy level structure. Excited electrons in higher energy levels combine with lower energy 'holes' and, upon recombination, emit single photons. Different options are possible for the creation of electron–hole pairs, including both optical (e.g. through an external laser field) and electrical excitations of electrons. Distribution Bragg reflection (DBR) mirrors can be introduced to couple the emission of emitted photons into a particular direction and increase generation rates. While photons can be released efficiently and controllably, quantum dots require cryogenic temperatures to function, and the properties of the emitted photons depend heavily on how the quantum dot is manufactured (which is not precisely controllable). To this end, the tunability of the properties of emitted photons is an area of ongoing research.

A final example for the deterministic generation of single photons is via colour centres [Kurtsiefer et al., 2000]. A diamond lattice is adapted to include a point–defect, consisting of a nitrogen atom and an adjacent vacancy (i.e. replacing the carbon atoms in the lattice), known as an NV colour centre. The system can be excited and stimulated into emission to release a single photon. Often the lattice involves alternative meta-stable atomic states, which temporarily prevent the atom from undergoing stimulated emission, thereby decreasing the generation rate. NV colour centres release photons at 637nm with photon bandwidths close to 100MHz. However, these properties can be adapted by using alternative colour centres, for example a nickel–nitrogen–vacancy centre emits photons of 800nm with much narrower bandwidths of around 0.5MHz. This level of control is desirable, although some systems require cryogenic temperatures and, as is the case with quantum dots, precise repeatability of photons emitted from separate colour centres is difficult to attain.

Probabilistic single photon generation derives from a range of different physical mecha-

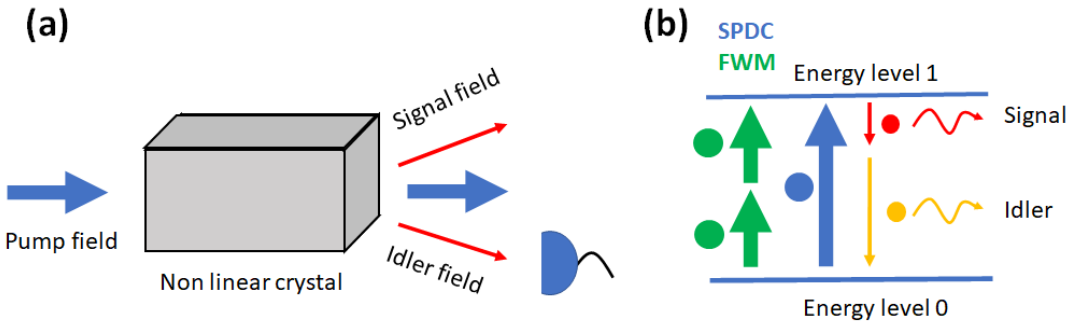

Figure 15: Non–linear interactions as a method of generating single photons. (a) A classical pump field causes a signal and idler field to evolve out of the vacuum state into a two mode squeezed state. (b) Photon picture of spontaneous parametric down conversion involving one pump photon, and four wave mixing, involving two pump photons of half the energy.

nisms. Single photons can be generated through non–linear interactions. In a method known as *spontaneous parametric down conversion* (SPDC) a strong classical pump field is applied to a second–order non–linear crystal, promoting two new fields, known as the signal and idler, from the vacuum via a quantum effect. As an aside, this mechanism is a deterministic route to generating *squeezed states* which are states of the form $|\psi\rangle = \lambda |00\rangle + \lambda^2 |11\rangle + \lambda^3 |22\rangle + ...$, where the kets give the number of photons in each of the signal and idler fields, and $\lambda < 1$ is a normalisation constant known as the *squeezing parameter*. Squeezed states can be used directly for continuous variable quantum protocols, and the degree of squeezing is given by λ [Lvovsky, 2016].

Alternatively, a single photon can be probabilistically generated in the signal field by measuring the idler field with a single photon detector. In the instance where the measurement outcome from $M_1 = |1\rangle\langle 1|$ is attained on the idler field, then the squeezed state is updated $|\psi\rangle \rightarrow |11\rangle$ with probability λ^2. The idler field is destroyed upon measurement, but the system is left in a single photon state in the signal field. This technique is often used in bulk, table–top quantum optics experiments because of its feasibility – it is cheap, simple and can operate at room temperature. Key drawbacks beyond the probabilistic generation, are that the wavelengths of light generated are limited by the non–linear crystal used, and often measurements project the signal field into a multi–photon subspace. By engineering the pump field, and in some instances, introducing a cavity structure, the outputted single photons can achieve a high degree of purity. In the photon picture, one pump field photon converts into one signal and one idler field photon (see figure 15), where the energy before and after the non–linear interaction is conserved.

A similar effect is *four wave mixing*, which involves a third–order non–linear interaction. In the photon picture, two pump field photons cause an excitation and generate a squeezed state in the outputted signal and idler fields. Since most materials have third–order non–linear coefficients, this effect has been demonstrated in a range of mediums, including directly inside

optical fibres and waveguides [Sharping et al., 2001].

Mechanism	Temp (K)	Wavelength	Tunability	Bandwidth	Spatial mode
Atom	~ 0	transition	fm	20 fm	single
Ion	~ 0	transition	fm	10 fm	single mode
Colour centers	300	640–800 nm	nm	nm	multimode
Quantum Dots	200	340–370nm	nm	nm	multimode
SPDC	300	vis / IR	nm	nm	multimode
FWM	300	vis / IR	nm	nm	single

Table 2: Generation mechanisms. Atom and ion tunability and bandwidths based on emitted photon wavelength of 750nm. Bandwidth in this context refers to the typical bandwidth of the photon wavepacket generated by a particular physical mechanism – this should be matched to control photon interaction with various components in a quantum communication system.

4.3.2 Information transmission

After generating states which contain quantum information, it is necessary to transmit them across a communication network. In optical quantum systems, loss, decoherence and state errors are key challenges which need to be overcome.

As mentioned earlier in the report, as light travels it naturally attenuates. A naive model of optical loss considers a classical plane wave, with wavelength λ, travelling through a medium of complex refractive index $n = n^{'} + in^{''}$, in the z direction. By solving Maxwell's equations, it can be show that,

$$|E(z)|^2 = |E(z=0)|^2 e^{-\alpha z} \tag{85}$$

$$\alpha = \frac{4\pi n^{''}}{\lambda}$$

and therefore it can be seen that the intensity of the light decreases exponentially with the distance travelled. The same is true in the quantum case for single photons. In this instance, it is the *probability* for the detection of the single photon which decays exponentially with distance, rather than the (classical) electric field. This gives rise to a decibel measure of loss, given by

$$dB = 10 \log_{10} \left(\frac{P}{P_0} \right) \tag{86}$$

where P and P_0 are the final (i.e. detected) and initial powers of the classical electric field. In the quantum case, this is replaced by the initial probability of detecting a photon (close to 1) and the probability of detection at some later distance. This can be used to answer how far single photons can be transmitted.

Considering direct transmission, state of the art optical fibres have losses of around 0.14 dB/km [Tamura et al., 2018, Hasegawa et al., 2018], and so the probability a single photon survives transmission across 500km is 10^{-7} [Gisin, 2015]. With sufficiently high generation rates of 1 GHz (i.e. the generation of 10^9 single photons per second), and high detection efficiencies

close to 100%, this could feasibly yield a detection of 100 photons per second – although, it should be noted that these parameters are beyond the means of current technologies, which are limited by a 100km range. If sufficient resources were available, it would in principle be possible to transfer quantum information in parallel (often known as single–photon multiplexing) to increase the photon generation rate, and associated communication rate; if each photon contains a qubit, parallel generation allows for a linear increase in the number bits of information that could be transferred. This would require generation, transmission and detection resources to be increased. For instance, if all generators – limited by single photon generation rates – transmission routes – limited e.g. by the number of photons that could be fitted into time bins along a path in a time–bin encoded scheme – and detectors – limited by their dead times (see next section) – were at full capacity, then a doubling of transferred qubits would require a doubling of each of these components.

Direct transmission of photons across free space can also be considered. In this case, akin to wireless communication, a similar calculation to above can be performed – the loss (for ground-to-ground communication) is much larger and so direct transmission of single photons turns out to be impractical. In the classical case, high energy radio frequency waves are often used for wireless communication which overcome loss limitations. This is not possible for transmission of single photons, which have a (comparatively) small energy, proportional to the photon's frequency. Loss levels for ground-to-space communications are much lower, and so do offer a viable route to implement free space transmission.

Engineering improvements to optical fibre loss, photon generation rates and detection efficiencies offer one route to improve transmission distances; although this yields diminishing returns because loss is exponential. An alternative is to apply quantum theory directly, through the use of quantum memories and repeaters, which is outlined in the next paragraph (see also §3.5).

Entanglement and the teleportation protocol can act as 'quantum repeaters' which increase the transmission distance [Ruihong and Ying, 2019]. In this method, a large distance is divided into a set of smaller parts and the photon is teleported across each section in turn. This requires nodes at each section to share entanglement. Naively, a series approach could be considered – entangling the first section with the second and teleporting quantum information between them, followed by the second section with the third, and so on – but this approach turns out to be inefficient. Instead, creating shared entanglement between sections in parallel is required. This introduces the need for quantum memories because performing many simultaneous entangling operations is unlikely to be successful (with the likelihood exponentially decreasing with the number of sections). Instead, adjacent sections can be made to develop entanglement independent of entanglement in other sections, gradually building up entanglement across the whole network. Once all the sections have generated shared entanglement, quantum information can be teleported across the transmission distance without suffering the effects of exponential loss. The teleportation protocol offers its own set of challenges however.

The physical implementation of quantum information transmission has developed rapidly in recent times, although further development is required before the transmission distances

surpass the 500km bound (roughly the limit of direct photon transmission with near-term technologies). This will arise from the development of quantum memories and repeaters. At present, entanglement of photons across distances of 96 km in telecom optical fibre has been demonstrated [Wengerowsky et al., 2019], although genuine repeater–based systems are impractical until quantum memory times increase. Current state of the art memories allow storage of quantum information over the order of milliseconds, while it is expected that this will need to increase to the order of seconds to be useable in a quantum communication network [Bhaskar et al., 2020, Wallucks et al., 2020].

While ground to ground communications are performed with optical fibres, an alternative option is to employ free–space ground–satellite links. Compared to ground–ground implementations, this option mitigates losses due to atmospheric noise and absorption [Aspelmeyer et al., 2003] because photons mainly (beyond 10km above sea level) travel in an environment similar to vacuum. In addition the atmosphere is less likely to induce errors in polarisation encoded qubits compared to fibre links. Although technology is not mature enough to use repeater based systems, satellite links have been used to demonstrate quantum information transmission over the range of 1000 km at reasonable transfer rates [Yin et al., 2020]. Note that, distances of up to 7000 km have been demonstrated, although the transfer rate of single photons is limited to 1 photon every 200s [Dequal et al., 2016].

In addition to loss (e.g. see figure 12 for photon loss as a function of wavelength), errors to the quantum information occur along transmission. For example, optical fibres distort the polarisation superpositions of qubits and inefficient detectors degrade qubits in teleportation protocols. In the near–term, both loss and qubit errors will be corrected by a combination of technological advances, e.g. the improvement of polarisation-maintaining fibres, and the implementation of new schemes and error correction codes, e.g. for use in satellite based communication [Muralidharan et al., 2016, Wu et al., 2020]. Typically, specific quantum error correction codes will be needed because classical error correction codes require measurements which disrupt (and potentially destroy) the quantum information that is being communicated; this is a rich field with ongoing research. For instance, continuous variable quantum information error correcting codes offer advantages in correcting photon loss while discrete variable surface codes use multiple photons to encode qubits; these both require photon redundancy. In trying to achieve the capacity of a given communication channel, there is often a trade-off between the redundancy of photons used to encode quantum information, against the robustness against photon loss and qubit errors.

4.3.3 Photon detection

Following the transmission of states through a quantum channel, they need to be measured in order to retrieve useful information. In this section, given the focus on single photon states, there is a review of photon detection systems, focusing particularly on their implementation and feasibility. As with photon state generation, there is a set of key parameters which define how well a detector performs.

- Detection efficiency: this is the probability that a photon, upon hitting the detector, triggers an electrical signal and thus yields a successful measurement. Ideally this should be 100%, but, in practice, this is reduced due to photon loss and imperfect photon coupling in the detector system.
- Dark-count rate: this is the rate at which electrical signals are generated in the absence of a photon hitting the detector; thereby giving the impression that a photon is present, when in reality it is not – this rate should be minimised for ideal detectors.
- Dead time: after a photon hits the detector, the dead–time indicates how long the detector needs to be able to detect another photon (it can't do so while it processes). Again, this should be minimised, and is especially important when the frequency of incident photons arriving at the detector is high. The inverse of the dead time yields the count rate of the detector.
- Jitter: this is the variation in time between a photon hitting the detector and an electrical signal being produced. Large variations create higher levels of uncertainty on the time the photon hits the detector. This is problematic if the uncertainty is larger than the time separation between consecutive detections – in this instance, these measurements could not be distinguished. Ideally there should be no variation.
- Photon number resolution: in some instances, as well as being able to distinguish between zero photons ($|0\rangle$) and one photon ($|1\rangle$), detectors can measure the number of photons hitting them (e.g. $|2\rangle$, $|3\rangle$ ...). This is especially useful for continuous–variable applications, for example when detecting squeezed states, which have state components with high photon numbers.

In the quantum regime, single photon detectors perform *measurements* of the photon's quantum state. This collapses the photon to a classical state e.g. for photons in a superposition of time-bins, the measurement collapses the photon to a particular position in time. While the focus in this chapter is on detecting the presence of a single photon (i.e. the detector clicks if a photon is present), there are mechanisms for detectors to determine the properties of a photon. For example, in the case of spatially encoded photons, detectors on each spatial mode will determine which route the photon is detected in, while the use of polarising filters can be used to determine a photon's polarisation. In this case, single photons are *destroyed* upon measurement; they can no longer undergo any further evolutions. This is distinct from the classical case, where upon being probed, classical light can be enhanced using amplifiers along transmission. In the quantum regime, careful consideration of the trade–off between measurement and single-photon destruction is required.

Also of significance, is the requirement of cryogenic temperatures for certain single photon detectors (most notably, the ones that can distinguish between different numbers of photons). This is a feature of quantum detectors because the energy of a photon needs to be filtered from background disturbances (which are typically energetically larger). This can add engineering complexity to quantum detection systems.

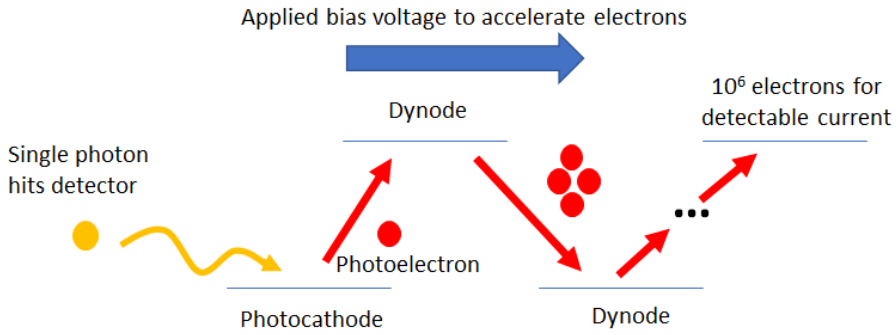

Figure 16: Diagram of a photomultipler tube. A single photon excites a photoelectron which is subsequently accelerated under an applied voltage. This causes a build up of electrons, which results in a detectable current.

The most primitive system of photon detection is via the photomultiplier tube (PT), as shown in figure 16. When a photon hits the detector (photocathode), it promotes a low energy 'photo–electron' which is subsequently accelerated by an applied voltage. The electron hits a dynode, releasing higher numbers of secondary electrons, and this process repeats over a set of dynodes. Eventually a pulse of around 10^6 electrons is generated, and this can be detected by ordinary electronic circuits, thus indicating a photon has hit the detector. Importantly this process takes place in vacuum, thus requiring technology which can limit their scalability and lifetime.

Improvements on the photomultiplier tube have been made – a key example is the single photon avalanche photodiode (SPAD). The basic outline of the physical mechanism is much the same as the photomultiplier tube, but an incident photon creates an electron–hole pair in a semiconductor material, which has a bias voltage applied across the semiconductor lattice (rather than to the vacuum). The subsequent charge build up (electron avalanche), is quickly saturated, set by the bias voltage, and this can be detected by electronics. While the detection efficiency of SPADs are higher than photomultiplier tubes, jitter and dark count rates are typically worse. The dead–time of SPADS is significant, and time is required for the system to reset before subsequent photon detection can be performed.

An alternative way to detect single photons is via superconducting nanowire single photon detectors (SNSPDs) [Gol'Tsman et al., 2001]. In this case, a thin wire of around 100nm is cooled into a superconducting state, which has extremely low electrical resistance. When a single photon hits the wire, the energy causes the incident area to move out of this state, thus creating a spot of higher resistance, and causing increased current density around the area's edges. Subsequently a whole area, the width of the wire, moves out of the superconducting state and has higher resistance, resulting in a voltage spike that can be interpreted as a photon count. While the jitter and dead–time in these systems are extremely low, key drawbacks are the temperature required (roughly 4K) and the fact that the detection area is very thin, and so

the detection efficiency is low. It is often the case that wires are meandered and placed in an optical cavity in order to increase the chances of a single photon hitting the wire.

The same technology can be used to act as a detector with photon number resolving capacities. In this instance, a set of separate wires are placed in close proximity in order to create a mesh of detectors. Sets of coincident voltage spikes indicate multiple photons hitting the detector [Divochiy et al., 2008].

A final example, which is photon number resolving, is the superconducting transition edge sensor (TES) [Cabrera et al., 1998]. Its mechanism is similar to SNSPDs, although it principally works on the basis that an incident photon will cause a change in the system's temperature. The detector has an extremely low heat capacity and is maintained in a superconducting state. When a photon hits the detector, it moves out of the superconducting state and its electrical resistance dramatically increases, resulting in a reduction of the electrical current flowing across it. The reduction in current is proportional to the number of photons hitting the detector. Detection efficiencies can be extremely high, reaching 95$\%$ in some instances, and the dark count rate is relatively low compared to alternative systems. However, key drawbacks are the fact that maintaining superconducting states requires low temperatures, typically TES's work at 100μK, and the dead times, which are around 100ns.

System	Efficiency	Temp (K)	Jitter	Dark count rate	Dead time
PT	40$\%$, λ =500nm	300	0.3ns	100 Hz	10^{-7} s
SPAD	65$\%$, λ =650nm	250	0.4ns	25 Hz	10^{-7} s
SNSPD	0.7$\%$, λ =1550nm	3	0.06ns	10 Hz	10^{-8} s
TES	50$\%$, λ =1550nm	0.1	100ns	3 Hz	10^{-5} s

Table 3: Detection mechanisms, including relevant parameters such as detection efficiency, operating temperature, jitter, dark count rate and dead time.

5 Current developments and implications

While the focus of this report has been on the possibility of developing technology beyond the limits of classical Shannon theory, this shorter section is devoted to understanding 'near term' implications of quantum theory for communication systems, including relevant case studies. Significant progress has been made in this field over the last decade, with small proof–of–principle quantum systems already being used in practice, demonstrating advantages in the security of the information transferred.

5.1 Current quantum communication networks

In the near-term, the main application of quantum networks is for quantum key distribution (QKD). The focus of this report is on medium-to-long term applications, so we will not discuss QKD in detail here, but will briefly discuss some current technological progress, which is relevant also to future applications of quantum networks.

Several QKD systems currently exist across the globe. In Britain, the Quantum Communications Hub aims to develop a large scale quantum network test-bed, involving both shorter–scale metropolitan networks in Cambridge and Bristol as well as a long–haul network connecting Cambridge–London–Bristol, with the scope to extend this. The Cambridge metropolitan network has already been developed, using already existing fibre links, demonstrating sucessful quantum key distribution in channels which have simultaneous data traffic of 100 Gbps; much of the infrastructure for this technology is already in place [Dynes et al., 2019].

To put the system in context, transfer of secure keys across fibre lengths of up to 10.6 km has been demonstrated, at a transfer rate of 2580 kbps. This was faithfully implemented across a period of 580 days.

The Chinese Academy of Sciences has demonstrated entanglement–enhanced QKD with the Micius satellite. Launched in 2016, it has facilitated space–to–ground quantum communication across distances of over 7500 km between China and Austria. This technology is still in its infancy, offering secure key transmission rates of just 0.43 bits per second, although further improvements are planned; notably the European–Asian and global encrypted networks which will develop over the coming decade [Bedington et al., 2017].

5.2 Random number generation

While strictly not limited to quantum communications systems, the generation of genuinely random numbers based upon the principles of quantum theory is reaching maturity and now backed by several quantum start–up companies [Herrero-Collantes and Garcia-Escartin, 2017]. These systems are truly random in the sense that data from them results from quantum effects, which are inherently random as described by quantum theory itself. This is distinct from many classical systems, where randomness derives from algorithmic complexity or fluctuations in the hardware – in this instance. For concreteness, if a user had enough knowledge about a classical

physical system (although this is often impractical), they could predict its behaviour. This is not the case in quantum mechanics – full understanding of the physical system would not allow for certainty about measurement results, because quantum state collapse is *inherently* random. Quantum random number generators could play a key role in QKD networks; one example being the choice of randomly prepared qubits used by Alice in the BB84 protocol – although this idea generalises to more practical protocols. Drawbacks of these systems include the limited generation rate and the need to verify the randomness of measured data – when convoluted with classical noise, it can be difficult to determine if the randomness produced is genuinely quantum.

Quantum random number generators can naturally be implemented in an optical setting. A range of options are available in this regime depending on how the quantum information is encoded in the photons. Branching path implementations encode information spatially, performing measurements with single photon detectors which are dependent upon the random collapse of quantum information caused by measurement. Alternatively, in a similar manner to time–bin encoded qubits, the time of arrival of a train of photons can be measured. The measurements here are, again, inherently random and the underlying random distribution can be controlled by manipulating the quantum properties of the light field in the system. The notion of squeezed states, which were described by a superposition of different numbers of photons can also be applied. If photon number resolving detectors are available, the number of photons measured at a detector upon the arrival of a squeezed state is, again, inherently random at the quantum level. Significant practical challenges remain in this field however, most notably the dead–time of detectors, which limits random number generation rates to Mbps.

5.3 Transmitting two bits with a single qubit: superdense coding

Superdense coding offers the possibility to transmit two classical bits of information by using only a single qubit and entanglement. This protocol is the inverse of quantum teleportation, which transmits two classical measurements in order to transfer a single qubit state [Bennett and Wiesner, 1992]. Superdense coding is an example of classical communication through quantum channels with the assistance of free entanglement – discussed in §3.2.2.

The general outline of the protocol involves Alice having access to one half of an entangled Bell state and applying a known unitary operation to encode the classical information she wishes to send. Bob has has access to the other half of the Bell state. After appropriately encoding classical information in the qubit, Alice sends her *single* qubit to Bob across a quantum channel. Bob can perform single qubit measurements on his initial qubit (half of the Bell state) and the one which was sent to him by Alice, which yields two bits of classical information – this information can be controlled by Alice via her choice of unitary at the start of the protocol. This protocol is also useful because it can offer security in a similar way to entanglement–enhanced QKD.

This protocol has been demonstrated experimentally in optical fibres, with a channel

capacity of 1.665 and a fidelity of 0.87, using hybrid time–polarisation encoded optical qubits. However, note that as discussed in §3.2.2, the scope of practical utility of superdense coding is at present unclear, as the generation of the shared entangled state is (and in most scenarios will likely continue to be) much more difficult to implement than simple adding an extra classical communication channel. However, there may indeed be specific examples where generating a shared entangled state at a time prior to communication is easier than sending a classical bit at the time of communication, in which case superdense coding could prove to be a very useful method which can increase the communication capacity of a given classical transmission line by up to a factor of two.

5.4 Quantum computing

A more long-term goal of quantum technologies is the development of universal quantum computers. While quantum computing is not the focus of this report, placing this goal in context gives an indication of the coming developments in quantum technologies over the next decade. Moreover, it is important to note that in order to do any communication using quantum physics at all, some form of quantum processor (simple quantum computer) is required in order to generate and process the information being sent.

While efforts are being made on a range of different physical platforms, photonics offers a promising route, with recent advances already demonstrating quantum advantage [Flamini et al., 2018]. Key to the photonics platform is that, in spite of whichever platform becomes most appropriate for quantum computation, communication of quantum information between nodes will almost certainly be transmitted through light fields; photons will definitely play a role in the future of quantum technology. This idea leads to the notion of a quantum internet, with quantum computers at nodes connected via quantum optical channels.

Various routes are possible in the photonic platform and many of the obstacles that apply to developing a fully functional quantum communication system are of importance for the development of quantum computers e.g. development in photon detection and generation. There is current research in both discrete and continuous encoding schemes, with a range of start–up companies drawing funding from the private sector to develop small scale, proof of principle technologies.

China is playing a prominent role in this field, with a recent demonstration of quantum advantage in a photonic setting in a collaboration between several institutions across the country [Zhong et al., 2020]. While the algorithm implemented has no direct uses, it acts a proof of principle, showing that quantum technology can genuinely perform computations which are impossible (exponentially hard) in the classical regime. This will quickly pave the way to more sophisticated algorithms which will have significant impacts on society – key examples being the Shor algorithm, which can factorise large numbers exponentially faster than classical counterparts, putting current cryptography methods at risk, and the Grover search algorithm which offers a quadratic speed up for sifting through data sets.

In the near term (5-10 years), where fully fault tolerant computation will not be feasible,

there will be the development of 'noisy intermediate–scale quantum' algorithms (NISQ), which build upon recent demonstrations of quantum advantage. This stage will offer devices consisting of hundreds (rather than millions) of noisy qubits, and could be applied to a range of areas including simulation of basic quantum chemistry and small optimisation problems.

6 Timeline of key advances past, present and future

6.1 Timeline of the past major advances in quantum technology

Here we provide a timeline of some of the major advances in quantum communication and related quantum technologies since the initiation of the field. The list of milestones presented here is by no means exhaustive, and the choice of inclusion or omission of particular results should not necessarily be taken as a judgement of their importance.

1984 C Bennett and G Brassard invent BB84 Protocol for QKD, proposing a concrete application of quantum theory for use in information security [Bennett and Brassard, 1984].

1985 D Deutsch proposes the notion of a universal quantum computer; a device which can perform a complete set of programmable quantum operations [Deutsch, 1985].

1991 A Ekert invents E91 Protocol for entanglement-based QKD, taking advantage of the non–local nature of quantum theory [Ekert, 1991].

1992 D Deutsch and R Josza propose a computational problem for which no classical deterministic solution exits but can be solved efficiently on a quantum computer [Deutsch and Jozsa, 1992].

1994 P Shor invents Shor's algorithm for polynomial time integer factorisation on a quantum computer, with potential uses in cryptography [Shor, 1994].

1994 I Cirac and P Zoller propose an experimental realisation of the controlled-NOT gate using trapped ions, paving the way for lab based experiments focused on the development of quantum technology [Cirac and Zoller, 1995].

1995 P Shor proposes the first protocols for quantum error correction, designed to mitigate the build-up of errors that occur in physical quantum systems [Shor, 1995].

1995 C Monroe and D Wineland demonstrate the first experimental realisation of a quantum logic gate — the controlled-NOT gate with trapped ions, using the Cirac-Zoller scheme [Monroe et al., 1995].

2001 Shor's algorithm implemented for the first time at IBM's Almaden Research Center and Stanford University, factoring the number 15. Although this could easily be implemented classically, this was an important milestone in demonstrating Shor's alogrithm in a genuinely quantum fashion [Vandersypen et al., 2001].

2003 Deutsch–Jozsa algorithm implemented on an ion-trap quantum computer at the University of Innsbruck. While this experimental demonstration held no advantage over classical systems, it was a further demonstration of a physical implementation of a quantum algorithm [Gulde et al., 2003].

2005 S L Braunstein proposes the idea of continuous variable quantum information; setting a route for the encoding quantum states beyond the qubit regime [Braunstein and Van Loock, 2005].

2007 Researchers in Austria achieve entanglement-based photonic quantum key distribution through free space over 144 km, breaking an important milestone for the development of industrial QKD systems [Schmitt-Manderbach et al., 2007].

2014 Proposal to use squeezed light at LIGO to enhance detection capabilities and discover gravitational waves [Chua et al., 2014]. This was subsequently achieved two years later in 2016.

2016 Micius quantum communication satellite launched by the Chinese Academy of Sciences, dramaticallly increasing the range of which QKD could be implemented physically [Liao et al., 2017].

2018 Intercontinental quantum network link established between China and Austria, achieving QKD over 7600 km relayed via the Micius satellite, far surpassing distances over which QKD had previously been demonstrated [Liao et al., 2018].

2019 Google's quantum computing team claim to have reached 'quantum supremacy' – that is the demonstration of a task impossible to simulate classically – using their 53-qubit Sycamore processor [Arute et al., 2019].

2020 Scientists unveil an eight-user metropolitan quantum communication network in Bristol, using fibres already deployed, hence taking advantage of existing classical communications systems [Joshi et al., 2020].

2020 Scientists in China claim to have achieved quantum supremacy using the photonic system Jiuzhang, which has a peak of 76 and average of 43 qubits, by performing calculations 100 trillion times faster than would be possible using a classical supercomputer [Zhong et al., 2020].

2021 An integrated space-to-ground quantum communication network over 4,600 kilometres is completed in China, enabling QKD to be performed reliably by multiple users across the network without the need for quantum repeaters [Chen et al., 2021].

2021 First demonstrations of a programmable, continous–variable photonic quantum chip, which may act as a 'launchpad' for scaling photonic quantum systems [Arrazola et al., 2021].

2021 Researchers in the EU present the first prototype of a distributed quantum computer, by performing a quantum-logic gate between quantum-network modules connected via a 60-metre-long optical fibre [Daiss et al., 2021].

6.2 Roadmap of the possible evolution of quantum networks

Here we present a roadmap showing the different stages in the future development of quantum communication networks, based on recent academic and industrial reviews [Wehner et al., 2018, Acín et al., 2018, Innovate UK and EPSRC, 2015]. A rough estimate of the timeline to commercialisation in the next 5-10 years is given. However, there is no agreed upon consensus for the time frame after that, so the stages are simply presented in the order that they will become commercialised. Each stage presents a fundamentally novel type of network, which includes the functionalities of all those below it.

Some notes on the terminology used in the roadmap: *Few-qubits* means that the number of qubits in each processor is still below the limit of qubits which can be efficiently simulated on a classical computer. *Blind quantum computation* refers to using remote quantum servers without revealing to the server what is being computed.

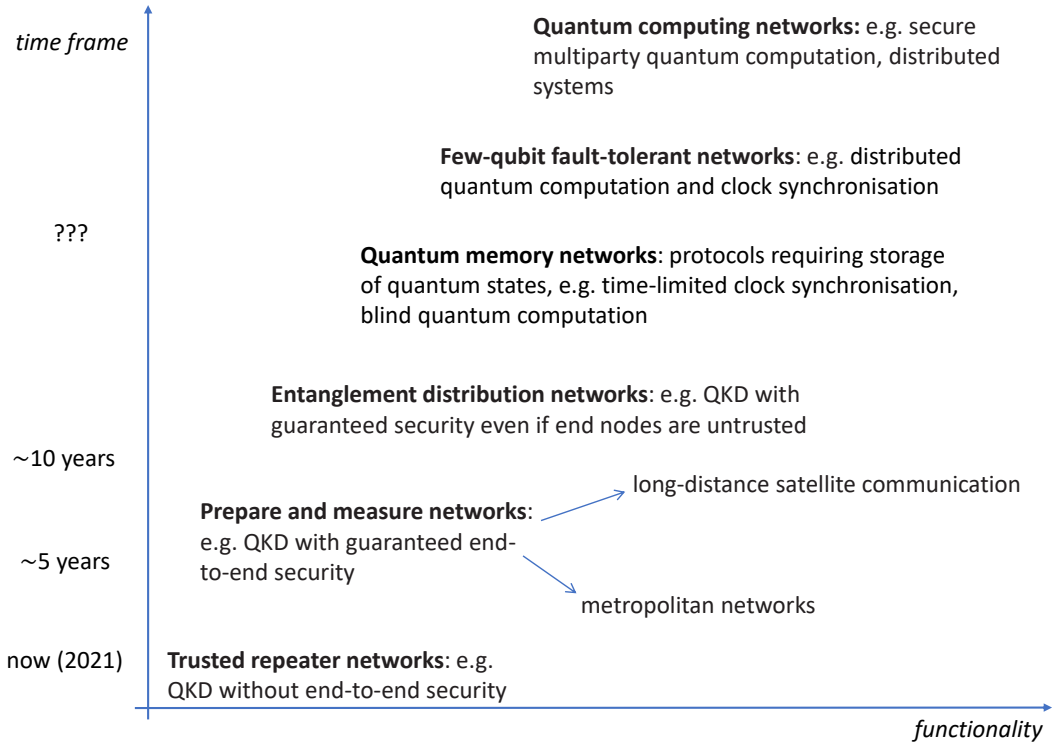

Figure 17: A graph of the various stages in the future development of quantum communication networks, with the possible time frames until commercialisation on the vertical axis and functionality on the horizontal axis.

7 Current industry standards

With quantum communications and cryptography technologies being developed for various applications by different players across the world, it is important that the industry forms internationally recognised standards.

The ETSI (European Telecommunications Standards Institute) is currently working on developing standards for QKD – the quantum communications technology currently closest to commercialisation. This includes a working group know as the ETSI Industry Specification Group (ISG) on QKD, whose membership consists of '*large companies, telecom operators, SMEs, NMIs, government labs and Universities and has representatives from North America, Asia and Europe*' [ETSI, 2021b]. The ISG has published two white papers: 'Implementation Security of QKD' [ETSI, 2018] and 'Quantum Safe Cryptography and Security' [ETSI, 2015], as well as a series of technical reports which precisely define and standardise the technical terms and protocols to be used for QKD [ETSI, 2021a].

The ETSI also has a Cyber Quantum Safe Cryptography (QSC) Working Group which assesses and makes recommendations for designing and implementing cryptographic protocols resistant to quantum attacks [ETSI, 2021c]. The QSC working group has published a technical report with standardised guidance on migrating from current security infrastructure to a fully quantum-safe one [ETSI, 2020]. The ETSI does not however appear to be working on concrete standards for quantum-safe protocols in the same way as for QKD.

The ETSI does not appear to have much work on standards for quantum communication technologies more general than QKD. However, it can be envisaged that the standards for the quantum communications networks necessary to implement QKD could be readily applied for further applications.

IEEE (The Institute of Electrical and Electronics Engineers) has an active project and working group on quantum communication standards, P1913 – Software-Defined Quantum Communication [IEEE, 2021].

The ITU (International Telecommunication Union) also has several working groups involved with quantum communication and related technologies, and have recently published a recommendation report 'Overview on networks supporting quantum key distribution' [ITU, 2019b]. In a 2019 article on their website, they write:

'*Network aspects of quantum information technologies are under study in ITU-T Study Group 13 (Future networks). The security dimensions of these technologies are under study in ITU-T Study Group 17 (Security). ITU has also established an open-to-all Focus Group on 'Quantum Information Technology for Networks' to study the evolution of these technologies in view of their foreseen applications in ICT networks.*' [ITU, 2019a]

8 Major industrial and academic players

A large number of private companies around the world are currently working on quantum communications. These companies are primarily based in Japan, China, the EU and Switzerland, and the USA. A comprehensive (although not exhaustive) list of private companies can be found in the 2018 Science for Policy report by the Joint Research Centre (JRC) of the European Commission, Chapter 3.2 [Lewis and Travagnin, 2018]. This list also includes a small number of public research institutions directly involved with real-world applications.

The UK is home to the Quantum Communications Hub, a consortium of private companies and academic research groups involved in the research and development of quantum communications systems in practice. A full up-to-date list of principal investigators (many of whom are heads of research groups at their respective institutions) can be found on the Hub's website: `https://www.quantumcommshub.net/research-community/about-the-hub/the-team/` A full list of the industrial partners is also available on the website at `https://www.quantumcommshub.net/research-community/about-the-hub/the-partnership/`

Theoretical research on the fundamental limits and possibilities of quantum communication is often carried out in research groups working on more general research programmes in quantum information theory. In these fields, applications of the same physical principle can often be applied to novel ideas in communication, computation, cryptography, as well as foundational research. Experimental work on quantum devices and implementation of specific elements of a technology are similarly often carried out in research groups that do not specifically focus on communication but build quantum devices for general quantum technologies, which only at the commercialisation stage are taken up by the more industrially-oriented players. A comprehensive and unbiased list of the key theoretical or experimental research groups in early-stage research is therefore difficult, if not impossible, to produce.

9 Conclusion

In this report, we have seen how quantum physics enables the possibility of developing a new generation of communications technologies.

9.1 Summary

This report began with an overview of the basics of quantum theory in the context of communication, highlighting phenomena such as superposition and entanglement, which radically distinguish quantum physics from its classical counterpart. This was followed by an introduction to the basics of quantum communication in practice. The main types of communication scenarios were discussed, highlighting the fact that quantum comes with four different channel capacities corresponding to the communication of 1. classical information, 2. classical information with the assistance of shared entanglement, 3. private classical information, and 4. quantum information. Examples of common quantum channels were given, including both discrete channels (used in single-photon communication) and continuous-variable channels (more similar to classical channels), and the expressions for their various types of capacities were given.

Quantum networks were introduced, along with a discussion of their implementation, which will eventually consist of quantum repeaters and quantum memories, as well as key-use cases of distributed quantum computing, quantum cloud computing and ultra-precise clock synchronisation, motivating the development of a quantum internet. The novel paradigm of quantum communication with quantum control of transmission lines was also discussed, shedding light on the way in which quantum theory can apply not only to information transmission, but also to the configurations of the transmission lines themselves, with potential capacity advantages for the communication of both classical and quantum information illustrated. The technical challenges of implementing quantum communication in practice was discussed in detail, starting with a discussion of single photons. The various possible ways to encode information in photons was discussed, as well as the generation of quantum states by a sender, their transmission through noisy channels, and their various methods of detection by the receiver.

The last few chapters of the report explored some important applications of quantum communication, such as examples of current quantum communication networks, provided a timeline of past advances in the field and a roadmap for future developments, summarised the latest work on industry standards, and discussed some of the major industrial and academic players.

9.2 Quantum vs. classical

A reader familiar with classical communication systems may be interested in how and in what scenarios quantum technologies may eventually replace existing classical communication

systems. As pointed out throughout the report, we are unfortunately not yet at the technological stage where a concrete answer to this question can be given. In the short-to-medium term, we do not expect quantum technologies to directly compete with existing communication technologies, except perhaps for the case of QKD. Rather, quantum technologies provide completely new applications that can be expected to complement existing communication technologies. For example, quantum computers are able to perform certain types of calculations much more efficiently than classical computers, yet, are not practical for use in day-to-day computing. Quantum computers operate on qubits instead of bits, and thus need to be connected via quantum communication networks in order to perform joint computations, e.g. for distributed quantum computing or quantum cloud computing. Nonetheless, classical communication networks, operating on bits, will in the foreseeable future mostly likely continue to provide the same functions as they do now, such as wifi and fibre networks, alongside the new quantum networks performing new functions.

For these reasons, in many scenarios it is not possible to make a direct comparison between classical and quantum networks. The former does certain things very well, while the latter is designed to perform tasks not possible with the former, such as communication with guaranteed security or distributed quantum computing. However, for the task of communicating classical information, one could ask if, and to what extent, quantum methods can provide an advantage over classical methods (perhaps analogous to the question of to what extent TV channels can transmit radio programmes better than radio channels). Yet, even this is a difficult question to answer, because it depends on the point of comparison. The leading communications technologies using quantum methods are single photons and continuous-variable photonics. Single photons experience noise in a completely different way to classical optical waves, and their generation and detection involves completely different, and much more complicated techniques, which are not yet able to perform large-scale communication in the same way as classical systems. Therefore a comparison between using single photons vs. classical optics will have to wait until single photons mature in their technological level. Continuous-variable photonics admits a more similar description to classical optics, and therefore we have provided a theoretical comparison in §3.4. This showed that encoding information in quantum-specific states does not improve the classical capacity but decoding information using quantum photon detection methods does improve the classical capacity compared to classical only methods. Nevertheless, this comparison is purely theoretical, and until the technologies used to generate and detect quantum states reach greater maturity, the full practical usefulness of quantum methods for classical communication remains an open question.

Finally, we recall that superdense coding enables twice the number of bits to be sent between a sender and receiver, if they pre-share entangled states. This could be of great practical use, but only if there are practical situations in which pre-sharing entangled states is easier than communicating classical bits. Similarly, the quantum control of transmission lines promises the ability to reliably transmit information through extremely noisy channels. However, the practical usefulness depends on the difficult of performing this type of quantum control. Again, in both of these use-cases, the full potential remains to be seen as the technologies mature.

9.3 Outlook

At present, governments and private companies around the world have started building quantum communication networks, for the first large-scale commercial application of quantum communications, namely, quantum key distribution (QKD). QKD enables cryptographic security guaranteed by the laws of physics, in contrast to current cryptographic protocols which rely on ever-evolving assumptions on the computational power of the eavesdropper. QKD is essential for the long-term security of sensitive data, which already at present could be vulnerable to 'intercept-now-decrypt-later' attacks, with the advent of quantum computers able to break current cryptographic protocols. More generally, quantum theory enables the possibility of sending **private information** through ordinary transmission lines. That is, when information is encoded in quantum states, any transmission line has a *private capacity*, which gives the maximum rate at which bits which can both be sent to the receiver and be fundamentally inaccessible to anyone else. The private capacity of a transmission line can in general be realised without the need for key distribution; in the future users may be able to communicate through quantum networks with guaranteed known bounds on the privacy of their information.

In the medium and long-term, the use of quantum communication networks is expected to extend to a variety of commercial applications, such as **ultra-precise clock synchronisation, quantum cloud computing** and **distributed quantum computing**, culminating in the advent of a **quantum internet**. The quantum internet would allow quantum computers located at distant points on the globe to be interconnected via fully quantum transmission lines, which transmit **quantum information**, measured in qubits, instead of the ordinary classical information of bits. (Thus, the quality of a quantum transmission line will be measured by the *quantum capacity*, which quantifies the rate of sending qubits through the channel.) Quantum computers are promised to be able to solve computational problems that are intractable for ordinary classical computers, with applications ranging from cybersecurity to drug discovery. Connecting quantum computers via a quantum internet would allow them to work together to form even more powerful processors, in a similar way to how our current internet enables personal and industrial computers to communicate across the globe.

Once quantum communication networks are in place they can also be used for more traditional purposes, such as the transmission of ordinary classical information, for which quantum methods have, in certain scenarios, been shown to yield higher communication rates than purely classical ones, for example using superdense coding or quantum photon detection methods. However, before quantum networks can be realised in practice, many technological challenges will need to be overcome. With the current impetus in quantum research, and enough government funding, we can expect in the coming decades to have commercialised devices for the generation and detection of quantum states, as well as quantum repeaters and memories, powerful enough to operate large-scale quantum communication networks at metropolitan and international levels.

Glossary and comparison of quantum/classical terminology

Below is a selection of key terms used in the report. In instances where there is a difference between quantum and classical terminology for the same idea, the classical term is highlighted in bold in the description,

- Bandwidth: Channel bandwidth describes the amount of information that can be transferred per unit time. Photon bandwidth is a measure of the spread of frequencies that form a photon's spectrum.
- Bloch ball: this a geographical representation of a qubit's quantum state. In the case of photon polarisation it is the Poincaré sphere.
- Capacity (classical / private / quantum): the maximum number of bits (private bits / qubits) that can be transmitted through a quantum channel, per channel use, in the asymptotic limit of infinitely many uses. A *use* of a channel refers to sending a single symbol through the channel – in the case of 2-dimensional channels this corresponds to sending a single bit (private bit / qubit).
- Coherence: typically refers to **spectral** coherence i.e. the degree of to which a photon has predictable spectral phase. Coherence time and coherence length are the times and lengths over which a photon remains coherent. In the quantum setting, coherence can also refer to the degree to which a system remains 'quantum'; characterised by the off-diagonal components of a state's density matrix.
- Channel: A quantum channel is an evolution which takes one valid quantum state to an alternative valid quantum state (given through completely positive, trace preserving maps). In the context of communication, a quantum channel corresponds to a communication channel which can transmit quantum information, as well as classical information.
- Dirac notation: is used in quantum theory as a shorthand for describing quantum states and operations. Key components are 'kets' e.g. $|0\rangle$ which describe quantum states, and 'bras' e.g. $\langle 0|$, which can combine with kets to describe matrices e.g. $|0\rangle \langle 0|$.
- Density matrix: full formalism for describing a quantum state and given through a matrix. The diagonal components of the density matrix describe the classical components of a quantum state. For pure states, density matrices are often reduced to state vectors, which encode the same information.
- Dark count rate: regarding single photon detectors, this is the rate at which electrical signals are generated in the absence of a photon hitting the detector.
- Dead time: regarding single photon detectors, the dead–time indicates how long the detector needs in order to perform consecutive measurements. The inverse of the dead time yields the count rate of the detector

- Detection efficiency: this is the probability that a photon, upon hitting the detector, triggers an electrical signal and thus yields a successful measurement.
- Entanglement: this gives rise to correlations between measurements of sets of quantum systems which cannot be described with a classical framework.
- Evolution: describes a transformation from one (classical or quantum) state to another. Generalised evolutions are able to describe any physical transformation i.e. through quantum channels.
- Error: in quantum theory corresponds to any unwanted change in a photon's quantum state during evolution, e.g. for qubits, unwanted rotations around the Bloch Ball.
- Jitter: with regard to single photon detectors, this is the variation in time between a photon hitting the detector and an electrical signal being produced.
- Loss: typically refers to the loss of a photon along a communication channel. Also considered a type of error.
- Measurements: in quantum theory a measurement probes a quantum state, collapsing it to a classical one. For photonic systems, a measurement corresponds to the **detection** of a single photon.
- Memory: refers to (generically atomic) memories, which are used to store quantum information. This is important in quantum communication systems for setting up entanglement nodes.
- Noise: used interchangeably with error, in quantum theory corresponds to any unwanted change in a photon's quantum state (includes both what is known as **additive noise** and **multiplicative noise** in classical communications).
- Quantum state: gives a description of the quantum information stored in a system. Generally categorised into two classes: pure states, which are well defined and mixed states, which are a set of pure states with some classical uncertainty regarding which state the system is in. A two-dimensional quantum state is called a qubit.
- Qubit: this the quantum analogue of a **classical bit**. The distinction here is that qubits can be in superposition states, and can entangle with other qubits.
- Spatial mode: for a photon this can be internal, linking to a photon's angular momentum states, or external, relating to a photon's position in space or path travelled.
- Superposition: typically refers to the fact that quantum systems display wave-like phenomena. An example is that a photon (discrete particle) can travel down a superposition of (i.e. multiple) paths at the same time.
- Repeater: quantum repeaters are nodes in a communication network which let entanglement to be stored. This allows for a large communication network to be entirely connected through quantum entanglement.

References

[Abbott et al., 2020] Abbott, A. A., Wechs, J., Horsman, D., Mhalla, M., and Branciard, C. (2020). Communication through coherent control of quantum channels. *Quantum*, 4:333.

[Acín et al., 2018] Acín, A., Bloch, I., Buhrman, H., Calarco, T., Eichler, C., Eisert, J., Esteve, D., Gisin, N., Glaser, S. J., Jelezko, F., et al. (2018). The quantum technologies roadmap: a European community view. *New Journal of Physics*, 20(8):080201.

[Andersen et al., 2010] Andersen, U. L., Leuchs, G., and Silberhorn, C. (2010). Continuous-variable quantum information processing. *Laser & Photonics Reviews*, 4(3):337–354.

[Arakawa and Holmes, 2020] Arakawa, Y. and Holmes, M. J. (2020). Progress in quantum-dot single photon sources for quantum information technologies: A broad spectrum overview. *Applied Physics Reviews*, 7(2):021309.

[Arrazola et al., 2021] Arrazola, J., Bergholm, V., Brádler, K., Bromley, T., Collins, M., Dhand, I., Fumagalli, A., Gerrits, T., Goussev, A., Helt, L., et al. (2021). Quantum circuits with many photons on a programmable nanophotonic chip. *Nature*, 591(7848):54–60.

[Arute et al., 2019] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G., Buell, D. A., et al. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510.

[Aspelmeyer et al., 2003] Aspelmeyer, M., Jennewein, T., Pfennigbauer, M., Leeb, W. R., and Zeilinger, A. (2003). Long-distance quantum communication with entangled photons using satellites. *IEEE Journal of Selected Topics in Quantum Electronics*, 9(6):1541–1551.

[Barros et al., 2009] Barros, H., Stute, A., Northup, T., Russo, C., Schmidt, P., and Blatt, R. (2009). Deterministic single-photon source from a single ion. *New Journal of Physics*, 11(10):103004.

[Bedington et al., 2017] Bedington, R., Arrazola, J. M., and Ling, A. (2017). Progress in satellite quantum key distribution. *npj Quantum Information*, 3(1):1–13.

[Bennett and Brassard, 1984] Bennett, C. H. and Brassard, G. (1984). Quantum cryptography: public key distribution and coin tossing. In *Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984)*, pages 175–9.

[Bennett et al., 1996] Bennett, C. H., DiVincenzo, D. P., Smolin, J. A., and Wootters, W. K. (1996). Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5):3824.

[Bennett et al., 1999] Bennett, C. H., Shor, P. W., Smolin, J. A., and Thapliyal, A. V. (1999). Entanglement-assisted classical capacity of noisy quantum channels. *Physical Review Letters*, 83(15):3081.

[Bennett and Wiesner, 1992] Bennett, C. H. and Wiesner, S. J. (1992). Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Physical Review Letters*, 69:2881–2884.

[Bhaskar et al., 2020] Bhaskar, M. K., Riedinger, R., Machielse, B., Levonian, D. S., Nguyen, C. T., Knall, E. N., Park, H., Englund, D., Lončar, M., Sukachev, D. D., et al. (2020). Experimental demonstration of memory-enhanced quantum communication. *Nature*, 580(7801):60–64.

[Braunstein and Van Loock, 2005] Braunstein, S. L. and Van Loock, P. (2005). Quantum information with continuous variables. *Reviews of Modern Physics*, 77(2):513.

[Briegel et al., 1998] Briegel, H.-J., Dür, W., Cirac, J. I., and Zoller, P. (1998). Quantum repeaters: the role of imperfect local operations in quantum communication. *Physical Review Letters*, 81(26):5932.

[Buller and Collins, 2009] Buller, G. and Collins, R. (2009). Single-photon generation and detection. *Measurement Science and Technology*, 21(1):012002.

[Cabrera et al., 1998] Cabrera, B., Clarke, R., Colling, P., Miller, A., Nam, S., and Romani, R. (1998). Detection of single infrared, optical, and ultraviolet photons using superconducting transition edge sensors. *Applied Physics Letters*, 73(6):735–737.

[Caleffi et al., 2018] Caleffi, M., Cacciapuoti, A. S., and Bianchi, G. (2018). Quantum internet: From communication to distributed computing! In *Proceedings of the 5th ACM International Conference on Nanoscale Computing and Communication*, pages 1–4.

[Chen et al., 2021] Chen, Y.-A., Zhang, Q., Chen, T.-Y., Cai, W.-Q., Liao, S.-K., Zhang, J., Chen, K., Yin, J., Ren, J.-G., Chen, Z., et al. (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, 589(7841):214–219.

[Chiribella, 2020] Chiribella, G. (2020). Quantum mechanics lecture notes.

[Chiribella et al., 2021] Chiribella, G., Banik, M., Bhattacharya, S. S., Guha, T., Alimuddin, M., Roy, A., Saha, S., Agrawal, S., and Kar, G. (2021). Indefinite causal order enables perfect quantum communication with zero capacity channels. *New Journal of Physics*, 23(3):033039.

[Chiribella et al., 2009] Chiribella, G., D'Ariano, G., Perinotti, P., and Valiron, B. (2009). Beyond quantum computers. *arXiv preprint arXiv:0912.0195*.

[Chiribella et al., 2013] Chiribella, G., D'Ariano, G. M., Perinotti, P., and Valiron, B. (2013). Quantum computations without definite causal structure. *Physical Review A*, 88(2):022318.

[Chiribella and Kristjánsson, 2019] Chiribella, G. and Kristjánsson, H. (2019). Quantum Shannon theory with superpositions of trajectories. *Proceedings of the Royal Society A*, 475.

[Chiribella et al., 2020] Chiribella, G., Wilson, M., and Chau, H. (2020). Quantum and classical data transmission through completely depolarising channels in a superposition of cyclic orders. *arXiv e-prints*, pages arXiv–2005.

[Chua et al., 2014] Chua, S., Slagmolen, B., Shaddock, D., and McClelland, D. (2014). Quantum squeezed light in gravitational-wave detectors. *Classical and Quantum Gravity*, 31(18):183001.

[Cirac and Zoller, 1995] Cirac, J. I. and Zoller, P. (1995). Quantum computations with cold trapped ions. *Physical Review Letters*, 74(20):4091.

[Cover and Thomas, 2006] Cover, T. M. and Thomas, J. A. (2006). Elements of information theory, 2nd ed.

[Daiss et al., 2021] Daiss, S., Langenfeld, S., Welte, S., Distante, E., Thomas, P., Hartung, L., Morin, O., and Rempe, G. (2021). A quantum-logic gate between distant quantum-network modules. *Science*, 371(6529):614–617.

[Del Santo and Dakić, 2018] Del Santo, F. and Dakić, B. (2018). Two-way communication with a single quantum particle. *Physical Review Letters*, 120(6):060503.

[Dequal et al., 2016] Dequal, D., Vallone, G., Bacco, D., Gaiarin, S., Luceri, V., Bianco, G., and Villoresi, P. (2016). Experimental single-photon exchange along a space link of 7000 km. *Phys. Rev. A*, 93:010301.

[Deutsch, 1985] Deutsch, D. (1985). Quantum theory, the church–turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117.

[Deutsch and Jozsa, 1992] Deutsch, D. and Jozsa, R. (1992). Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, 439(1907):553–558.

[Divochiy et al., 2008] Divochiy, A., Marsili, F., Bitauld, D., Gaggero, A., Leoni, R., Mattioli, F., Korneev, A., Seleznev, V., Kaurova, N., Minaeva, O., et al. (2008). Superconducting nanowire photon-number-resolving detector at telecommunication wavelengths. *Nature Photonics*, 2(5):302–306.

[Dynes et al., 2019] Dynes, J., Wonfor, A., Tam, W.-S., Sharpe, A., Takahashi, R., Lucamarini, M., Plews, A., Yuan, Z., Dixon, A., Cho, J., et al. (2019). Cambridge quantum network. *npj Quantum Information*, 5(1):1–8.

[Ebler et al., 2018] Ebler, D., Salek, S., and Chiribella, G. (2018). Enhanced communication with the assistance of indefinite causal order. *Physical Review Letters*, 120(12):120502.

[Eisaman et al., 2011] Eisaman, M. D., Fan, J., Migdall, A., and Polyakov, S. V. (2011). Invited review article: Single-photon sources and detectors. *Review of Scientific Instruments*, 82(7):071101.

[Ekert, 1991] Ekert, A. K. (1991). Quantum cryptography based on bell's theorem. *Physical Review Letters*, 67(6):661.

[Erhard et al., 2018] Erhard, M., Fickler, R., Krenn, M., and Zeilinger, A. (2018). Twisted photons: new quantum perspectives in high dimensions. *Light: Science & Applications*, 7(3):17146–17146.

[ETSI, 2015] ETSI (2015). Etsi white paper no. 8: Quantum safe cryptography and security. Accessed 5th February 2021 from `https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf`.

[ETSI, 2018] ETSI (2018). Etsi white paper no. 27: Implementation security of quantum cryptography. Accessed 5th February 2021 from `https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf`.

[ETSI, 2020] ETSI (2020). Technical report tr 103 619 cyber; migration strategies and recommendations to quantum safe schemes. Accessed 5th February 2021 from `https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf`.

[ETSI, 2021a] ETSI (2021a). Industry specification group (ISG) on quantum key distribution for users (QKD). Accessed 5th February 2021 from `https://www.etsi.org/committee/1430-qkd`.

[ETSI, 2021b] ETSI (2021b). Quantum key distribution (QKD). Accessed 5th February 2021 from `https://www.etsi.org/technologies/quantum-key-distribution`.

[ETSI, 2021c] ETSI (2021c). Quantum-safe cryptography (QSC). Accessed 5th February 2021 from `https://www.etsi.org/technologies/quantum-safe-cryptography`.

[Fanizza et al., 2020] Fanizza, M., Kianvash, F., and Giovannetti, V. (2020). Quantum flags and new bounds on the quantum capacity of the depolarizing channel. *Physical Review Letters*, 125(2):020503.

[Flamini et al., 2018] Flamini, F., Spagnolo, N., and Sciarrino, F. (2018). Photonic quantum information processing: a review. *Reports on Progress in Physics*, 82(1):016001.

[Freer et al., 2017] Freer, S., Simmons, S., Laucht, A., Muhonen, J. T., Dehollain, J. P., Kalra, R., Mohiyaddin, F. A., Hudson, F. E., Itoh, K. M., McCallum, J. C., et al. (2017). A single-atom quantum memory in silicon. *Quantum Science and Technology*, 2(1):015009.

[Gariano et al., 2017] Gariano, J., Djordjevic, I., and Liu, T. (2017). Optimal wavelength selection for entangled quantum key distribution. In *2017 IEEE Photonics Conference (IPC)*, pages 721–722. IEEE.

[Ghafari et al., 2019] Ghafari, F., Tischler, N., Di Franco, C., Thompson, J., Gu, M., and Pryde, G. J. (2019). Interfering trajectories in experimental quantum-enhanced stochastic simulation. *Nature Communications*, 10(1):1–8.

[Gibney, 2020] Gibney, E. (2020). Quantum computer race intensifies as alternative technology gains steam. *Nature*, 587(7834):342–343.

[Giovannetti et al., 2004] Giovannetti, V., Guha, S., Lloyd, S., Maccone, L., Shapiro, J. H., and Yuen, H. P. (2004). Classical capacity of the lossy bosonic channel: The exact solution. *Physical Review Letters*, 92(2):027902.

[Gisin, 2015] Gisin, N. (2015). How far can one send a photon? *Frontiers of Physics*, 10(6):1–8.

[Gisin et al., 2005] Gisin, N., Linden, N., Massar, S., and Popescu, S. (2005). Error filtration and entanglement purification for quantum communication. *Physical Review A*, 72(1):012338.

[Gol'Tsman et al., 2001] Gol'Tsman, G., Okunev, O., Chulkova, G., Lipatov, A., Semenov, A., Smirnov, K., Voronov, B., Dzardanov, A., Williams, C., and Sobolewski, R. (2001). Picosecond superconducting single-photon optical detector. *Applied Physics Letters*, 79(6):705–707.

[Goswami et al., 2018] Goswami, K., Cao, Y., Paz-Silva, G., Romero, J., and White, A. (2018). Communicating via ignorance: Increasing communication capacity via superposition of order. *arXiv preprint arXiv:1807.07383*.

[Gottesman, 2010] Gottesman, D. (2010). An introduction to quantum error correction and fault-tolerant quantum computation. In *Quantum information science and its contributions to mathematics, Proceedings of Symposia in Applied Mathematics*, volume 68, pages 13–58.

[Guérin et al., 2019] Guérin, P. A., Rubino, G., and Brukner, Č. (2019). Communication through quantum-controlled noise. *Physical Review A*, 99:062317.

[Gulde et al., 2003] Gulde, S., Riebe, M., Lancaster, G. P., Becher, C., Eschner, J., Häffner, H., Schmidt-Kaler, F., Chuang, I. L., and Blatt, R. (2003). Implementation of the deutsch–jozsa algorithm on an ion-trap quantum computer. *Nature*, 421(6918):48–50.

[Guo et al., 2020] Guo, Y., Hu, X.-M., Hou, Z.-B., Cao, H., Cui, J.-M., Liu, B.-H., Huang, Y.-F., Li, C.-F., Guo, G.-C., and Chiribella, G. (2020). Experimental transmission of quantum information using a superposition of causal orders. *Physical Review Letters*, 124(3):030502.

[Hasegawa et al., 2018] Hasegawa, T., Tamura, Y., Sakuma, H., Kawaguchi, Y., Yamamoto, Y., and Koyano, Y. (2018). The first 0.14-db/km ultra-low loss optical fiber. *SEI Tech. Rev*, 86:18–22.

[Hastings, 2009] Hastings, M. B. (2009). Superadditivity of communication capacity using entangled inputs. *Nature Physics*, 5(4):255–257.

[Herrero-Collantes and Garcia-Escartin, 2017] Herrero-Collantes, M. and Garcia-Escartin, J. C. (2017). Quantum random number generators. *Reviews of Modern Physics*, 89(1):015004.

[Higginbottom et al., 2016] Higginbottom, D. B., Slodička, L., Araneda, G., Lachman, L., Filip, R., Hennrich, M., and Blatt, R. (2016). Pure single photons from a trapped atom source. *New Journal of Physics*, 18(9):093038.

[Holevo, 1973] Holevo, A. S. (1973). Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11.

[Holevo, 1998] Holevo, A. S. (1998). The capacity of the quantum channel with general signal states. *IEEE Transactions on Information Theory*, 44(1):269–273.

[Holevo et al., 1999] Holevo, A. S., Sohma, M., and Hirota, O. (1999). Capacity of quantum gaussian channels. *Physical Review A*, 59(3):1820.

[IEEE, 2021] IEEE (2021). IEEE quantum initiative support for standards. Accessed 5th February 2021 from `https://quantum.ieee.org/standards`.

[Innovate UK and EPSRC, 2015] Innovate UK and EPSRC (2015). A roadmap for quantum technologies in the uk. Accessed 10th March 2021 from `https://epsrc.ukri.org/newsevents/pubs/quantumtechroadmap/`.

[ITU, 2019a] ITU (2019a). New ITU standard for networks to support quantum-safe encryption and authentication. Accessed 5th February 2021 from `https://news.itu.int/new-itu-standard-networks-support-quantum-safe-encryption-authentication/`.

[ITU, 2019b] ITU (2019b). Overview on networks supporting quantum key distribution. Accessed 5th February 2021 from `https://www.itu.int/rec/T-REC-Y.3800-201910-I`.

[Jennings, 2019] Jennings, D. (2019). Advanced quantum information lecture notes.

[Joshi et al., 2020] Joshi, S. K., Aktas, D., Wengerowsky, S., Lončarić, M., Neumann, S. P., Liu, B., Scheidl, T., Lorenzo, G. C., Samec, Ž., Kling, L., et al. (2020). A trusted node–free eight-user metropolitan quantum communication network. *Science Advances*, 6(36):eaba0959.

[King, 2003] King, C. (2003). The capacity of the quantum depolarizing channel. *IEEE Transactions on Information Theory*, 49(1):221–229.

[Knill et al., 2001] Knill, E., Laflamme, R., and Milburn, G. J. (2001). A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52.

[Komar et al., 2014] Komar, P., Kessler, E. M., Bishof, M., Jiang, L., Sørensen, A. S., Ye, J., and Lukin, M. D. (2014). A quantum network of clocks. *Nature Physics*, 10(8):582–587.

[Kristjánsson et al., 2020] Kristjánsson, H., Chiribella, G., Salek, S., Ebler, D., and Wilson, M. (2020). Resource theories of communication. *New Journal of Physics*, 22(7):073014.

[Kristjánsson et al., 2020] Kristjánsson, H., Mao, W., and Chiribella, G. (2020). Witnessing latent time correlations with a single quantum particle. *arXiv preprint arXiv:2004.06090*.

[Kurtsiefer et al., 2000] Kurtsiefer, C., Mayer, S., Zarda, P., and Weinfurter, H. (2000). Stable solid-state source of single photons. *Physical Review Letters*, 85:290–293.

[Lamoureux et al., 2005] Lamoureux, L.-P., Brainis, E., Cerf, N., Emplit, P., Haelterman, M., and Massar, S. (2005). Experimental error filtration for quantum communication over highly noisy channels. *Physical Review Letters*, 94(23):230501.

[Lewis and Travagnin, 2018] Lewis, A. M. and Travagnin, M. (2018). The impact of quantum technologies on the EU's future policies – Part 2 Quantum communications: from science to policies. Accessed 3rd February 2021 from `https://publications.jrc.ec.europa.eu/repository/bitstream/JRC107386/jrc_report_quantumcommunications.pdf`.

[Li et al., 2009] Li, K., Winter, A., Zou, X., and Guo, G. (2009). Private capacity of quantum channels is not additive. *Physical Review Letters*, 103(12):120501.

[Liao et al., 2018] Liao, S.-K., Cai, W.-Q., Handsteiner, J., Liu, B., Yin, J., Zhang, L., Rauch, D., Fink, M., Ren, J.-G., Liu, W.-Y., et al. (2018). Satellite-relayed intercontinental quantum network. *Physical Review Letters*, 120(3):030501.

[Liao et al., 2017] Liao, S.-K., Cai, W.-Q., Liu, W.-Y., Zhang, L., Li, Y., Ren, J.-G., Yin, J., Shen, Q., Cao, Y., Li, Z.-P., et al. (2017). Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47.

[Lounis and Orrit, 2005] Lounis, B. and Orrit, M. (2005). Single-photon sources. *Reports on Progress in Physics*, 68(5):1129.

[Lukens and Lougovski, 2017] Lukens, J. M. and Lougovski, P. (2017). Frequency-encoded photonic qubits for scalable quantum information processing. *Optica*, 4(1):8–16.

[Lvovsky, 2016] Lvovsky, A. I. (2016). Squeezed light.

[Macchiavello and Palma, 2002] Macchiavello, C. and Palma, G. M. (2002). Entanglement-enhanced information transmission over a quantum channel with correlated noise. *Physical Review A*, 65:050301.

[Massa et al., 2019] Massa, F., Moqanaki, A., Baumeler, Ä., Del Santo, F., Kettlewell, J. A., Dakić, B., and Walther, P. (2019). Experimental two-way communication with one photon. *Advanced Quantum Technologies*, 2(11):1900050.

[Menicucci et al., 2006] Menicucci, N. C., Van Loock, P., Gu, M., Weedbrook, C., Ralph, T. C., and Nielsen, M. A. (2006). Universal quantum computation with continuous-variable cluster states. *Physical Review Letters*, 97(11):110501.

[Meyer et al., 2015] Meyer, H. M., Stockill, R., Steiner, M., Le Gall, C., Matthiesen, C., Clarke, E., Ludwig, A., Reichel, J., Atatüre, M., and Köhl, M. (2015). Direct photonic coupling of a semiconductor quantum dot and a trapped ion. *Physical Review Letters*, 114:123001.

[Michelberger et al., 2015] Michelberger, P., Champion, T., Sprague, M., Kaczmarek, K., Barbieri, M., Jin, X., England, D., Kolthammer, W., Saunders, D., Nunn, J., et al. (2015). Interfacing ghz-bandwidth heralded single photons with a warm vapour raman memory. *New Journal of Physics*, 17(4):043006.

[Monroe et al., 1995] Monroe, C., Meekhof, D. M., King, B. E., Itano, W. M., and Wineland, D. J. (1995). Demonstration of a fundamental quantum logic gate. *Physical Review Letters*, 75(25):4714.

[Muralidharan et al., 2016] Muralidharan, S., Li, L., Kim, J., Lütkenhaus, N., Lukin, M. D., and Jiang, L. (2016). Optimal architectures for long distance quantum communication. *Scientific Reports*, 6(1):1–10.

[Nielsen and Chuang, 2000] Nielsen, M. A. and Chuang, I. L. (2000). *Quantum Computation and Quantum Information*. Cambridge University Press.

[Piparo et al., 2020] Piparo, N. L., Hanks, M., Gravel, C., Nemoto, K., and Munro, W. J. (2020). Resource reduction for distributed quantum information processing using quantum multiplexed photons. *Physical Review Letters*, 124(21):210503.

[Procopio et al., 2019] Procopio, L. M., Delgado, F., Enríquez, M., Belabas, N., and Levenson, J. A. (2019). Communication enhancement through quantum coherent control of n channels in an indefinite causal-order scenario. *Entropy*, 21(10):1012.

[Procopio et al., 2020] Procopio, L. M., Delgado, F., Enríquez, M., Belabas, N., and Levenson, J. A. (2020). Sending classical information via three noisy channels in superposition of causal orders. *Physical Review A*, 101:012346.

[Raina and Srinivasa, 2014] Raina, A. and Srinivasa, S. G. (2014). Quantum communication over bit flip channels using entangled bipartite and tripartite states. In *2014 52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1368–1375. IEEE.

[Reck et al., 1994] Reck, M., Zeilinger, A., Bernstein, H. J., and Bertani, P. (1994). Experimental realization of any discrete unitary operator. *Physical Review Letters*, 73:58–61.

[Ren et al., 2017] Ren, J.-G., Xu, P., Yong, H.-L., Zhang, L., Liao, S.-K., Yin, J., Liu, W.-Y., Cai, W.-Q., Yang, M., Li, L., et al. (2017). Ground-to-satellite quantum teleportation. *Nature*, 549(7670):70–73.

[Rubino et al., 2021] Rubino, G., Rozema, L. A., Ebler, D., Kristjánsson, H., Salek, S., Guérin, P. A., Abbott, A. A., Branciard, C., Brukner, Č., Chiribella, G., et al. (2021). Experimental quantum communication enhancement by superposing trajectories. *Physical Review Research*, 3(1):013093.

[Ruihong and Ying, 2019] Ruihong, Q. and Ying, M. (2019). Research progress of quantum repeaters. *Journal of Physics: Conference Series*, 1237(5):052032.

[Salek et al., 2018] Salek, S., Ebler, D., and Chiribella, G. (2018). Quantum communication in a superposition of causal orders. *arXiv preprint arXiv:1809.06655*.

[Schmitt-Manderbach et al., 2007] Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, J. G., et al. (2007). Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters*, 98(1):010504.

[Schumacher and Westmoreland, 1997] Schumacher, B. and Westmoreland, M. D. (1997). Sending classical information via noisy quantum channels. *Physical Review A*, 56(1):131.

[Shannon, 1948] Shannon, C. E. (1948). A mathematical theory of communication. *The Bell system technical journal*, 27(3):379–423.

[Shapiro et al., 2005] Shapiro, J., Guha, S., and Erkmen, B. (2005). Ultimate channel capacity of free-space optical communications. *Journal of Optical Networking*, 4(8):501–516.

[Shapiro, 2009] Shapiro, J. H. (2009). The quantum theory of optical communications. *IEEE Journal of Selected Topics in Quantum Electronics*, 15(6):1547–1569.

[Shapiro, 2021] Shapiro, J. H. (2021). Personal communication.

[Sharping et al., 2001] Sharping, J. E., Fiorentino, M., and Kumar, P. (2001). Observation of twin-beam-type quantum correlation in optical fiber. *Optics Letters*, 26(6):367–369.

[Shor, 1994] Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee.

[Shor, 1995] Shor, P. W. (1995). Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52(4):R2493.

[Slussarenko and Pryde, 2019] Slussarenko, S. and Pryde, G. J. (2019). Photonic quantum information processing: A concise review. *Applied Physics Reviews*, 6(4):041303.

[Smith and Yard, 2008] Smith, G. and Yard, J. (2008). Quantum communication with zero-capacity channels. *Science*, 321(5897):1812–1815.

[Stebila et al., 2009] Stebila, D., Mosca, M., and Lütkenhaus, N. (2009). The case for quantum key distribution. In *International Conference on Quantum Comunication and Quantum Networking*, pages 283–296. Springer.

[Tamura et al., 2018] Tamura, Y., Sakuma, H., Morita, K., Suzuki, M., Yamamoto, Y., Shimada, K., Honma, Y., Sohma, K., Fujii, T., and Hasegawa, T. (2018). The first 0.14-db/km loss optical fiber and its impact on submarine transmission. *Journal of Lightwave Technology*, 36(1):44–49.

[Tan and Rohde, 2019] Tan, S.-H. and Rohde, P. P. (2019). The resurgence of the linear optics quantum interferometer — recent advances & applications. *Reviews in Physics*, 4:100030.

[Valivarthi et al., 2020] Valivarthi, R., Davis, S. I., Peña, C., Xie, S., Lauk, N., Narváez, L., Allmaras, J. P., Beyer, A. D., Gim, Y., Hussein, M., et al. (2020). Teleportation systems toward a quantum internet. *PRX Quantum*, 1(2):020317.

[Vandersypen et al., 2001] Vandersypen, L. M., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H., and Chuang, I. L. (2001). Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414(6866):883–887.

[Vitanov et al., 2017] Vitanov, N. V., Rangelov, A. A., Shore, B. W., and Bergmann, K. (2017). Stimulated raman adiabatic passage in physics, chemistry, and beyond. *Reviews of Modern Physics*, 89(1):015006.

[Wallucks et al., 2020] Wallucks, A., Marinković, I., Hensen, B., Stockill, R., and Gröblacher, S. (2020). A quantum memory at telecom wavelengths. *Nature Physics*, 16(7):772–777.

[Wang et al., 2021] Wang, P., Luan, C.-Y., Qiao, M., Um, M., Zhang, J., Wang, Y., Yuan, X., Gu, M., Zhang, J., and Kim, K. (2021). Single ion qubit with estimated coherence time exceeding one hour. *Nature Communications*, 12(1):1–8.

[Wehner et al., 2018] Wehner, S., Elkouss, D., and Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science*, 362(6412).

[Wengerowsky et al., 2019] Wengerowsky, S., Joshi, S. K., Steinlechner, F., Zichi, J. R., Dobrovolskiy, S. M., van der Molen, R., Los, J. W., Zwiller, V., Versteegh, M. A., Mura, A., et al. (2019). Entanglement distribution over a 96-km-long submarine optical fiber. *Proceedings of the National Academy of Sciences*, 116(14):6684–6688.

[Wilde, 2013] Wilde, M. M. (2013). *Quantum Information Theory*. Cambridge University Press.

[Wu et al., 2020] Wu, J., Zhang, L., Jia, J., Wang, T., Shu, R., He, Z., and Wang, J. (2020). Polarization-maintaining design for satellite-based quantum communication terminals. *Optics Express*, 28(8):10746–10759.

[Yang et al., 2016] Yang, S.-J., Wang, X.-J., Bao, X.-H., and Pan, J.-W. (2016). An efficient quantum light–matter interface with sub-second lifetime. *Nature Photonics*, 10(6):381–384.

[Yin et al., 2020] Yin, J., Li, Y.-H., Liao, S.-K., Yang, M., Cao, Y., Zhang, L., Ren, J.-G., Cai, W.-Q., Liu, W.-Y., Li, S.-L., et al. (2020). Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature*, 582(7813):501–505.

[Zhao et al., 2014] Zhao, L., Guo, X., Liu, C., Sun, Y., Loy, M., and Du, S. (2014). Photon pairs with coherence time exceeding 1 μs. *Optica*, 1(2):84–88.

[Zhong et al., 2020] Zhong, H.-S., Wang, H., Deng, Y.-H., Chen, M.-C., Peng, L.-C., Luo, Y.-H., Qin, J., Wu, D., Ding, X., Hu, Y., et al. (2020). Quantum computational advantage using photons. *Science*, 370(6523):1460–1463.

[Zhong et al., 2015] Zhong, M., Hedges, M. P., Ahlefeldt, R. L., Bartholomew, J. G., Beavan, S. E., Wittig, S. M., Longdell, J. J., and Sellars, M. J. (2015). Optically addressable nuclear spins in a solid with a six-hour coherence time. *Nature*, 517(7533):177–180.

A Technical aspects of quantum theory

A.1 Product and entangled states

The tensor product allows for a notion of *entanglement*. Quantum states written in the form

$$|\psi_N\rangle = |\psi_0\rangle \otimes |\psi_1\rangle \otimes ... \otimes |\psi_{n-1}\rangle \,, \tag{87}$$

are known as product states. However, these are only a subset of the total set of possible quantum states that can be formed by considering composite systems. Analogously to pure and mixed quantum states, entangled states are ones which are necessarily written as a sum of product states.

For example, for an N-partite system, entangled states are written as,

$$|\psi_{\text{entangled}}\rangle = \sum_{i=0}^{m} |\psi_0^{(i)}\rangle \otimes |\psi_1^{(i)}\rangle \otimes ... \otimes |\psi_{(n-1)}^{(i)}\rangle \tag{88}$$

where $m \geq 1$ and $|\psi_{\text{entangled}}\rangle$ cannot be be re-written in a form where $m = 0$. Entangled states have important properties which can be exploited for quantum communication, as outlined throughout the report.

Evolutions of states are represented by matrices (e.g. reversible unitary evolution or projective measurements). Again, only a subset of the total possible set of evolutions possible for composite systems is described as '*product gates*'. For example,

$$\hat{A}_{\text{product}} = \hat{A}_0 \otimes \hat{A}_1 \otimes ... \otimes \hat{A}_{n-1} \tag{89}$$

and, in analogy to entangled states, matrices that cannot be written in this form are known as '*interaction gates*', and cannot be thought of as products of evolutions acting independently on

different subsystems. Instead, interaction gates act simultaneously and in dependence upon sets of subsystems.

The canonical example of an interaction gate for a composite system of 2 subsystems is the CNOT gate, given by,

$$CNOT = |0\rangle \langle 0| \otimes \hat{I}_2 + |1\rangle \langle 1| \otimes \hat{X} \tag{90}$$

where $\hat{X}$ is the Pauli X matrix. For example, consider it acting on state $|\psi_c\rangle = |\psi_a\rangle \otimes |\psi_b\rangle$ with $|\psi_a\rangle = |0\rangle$. In this instance, CNOT does nothing to $|\psi_b\rangle$,

$$(CNOT)\,|\psi_c\rangle = (|0\rangle \otimes |\psi_b\rangle) \tag{91}$$

while if $|\psi_a\rangle = |1\rangle$ it acts with $\hat{X}$ upon $|\psi_b\rangle$,

$$(CNOT)\,|\psi_c\rangle = (|1\rangle \otimes \hat{X}\,|\psi_b\rangle) \tag{92}$$

Gates such as these, which act on condition of particular states, become even richer when $|\psi_a\rangle$ is extended beyond $|0\rangle$ and $|1\rangle$ to genuine quantum superposition states.

Of interest is the fact that interaction gates can evolve product states into entangled ones. If the example above is generalised to allow a genuine quantum superposition in system 'a', $|\psi_a\rangle = |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, and a classical state in system 'b', $|\psi_b\rangle = |0\rangle$, it can be shown that,

$$(CNOT)(|+\rangle \otimes |0\rangle) = |\Phi_0\rangle \tag{93}$$

which is the Bell state. This means the evolution CNOT has transformed the product state, $|+\rangle \otimes |0\rangle$, to an entangled state, $|\Phi_0\rangle$. Interaction gates are thus useful in the sense that they allow systems to increase their entanglement, which is a useful resource in quantum communication protocols.

A.2 Quantum teleportation

A key use of entangled states is for quantum teleportation. The idea is to transport the (unknown) state of one qubit from one system to another which may not necessarily be in direct contact. This process requires entanglement.

Consider the situation of a three part composite system $|\Psi_{\text{init}}\rangle = |\psi\rangle \otimes |\Phi_0\rangle$, an unknown qubit in system 1 and a Bell state entangled across systems 2 and 3. The idea here is to entangle systems 1 and 2 (which could be brought into contact) and measure each of these systems. This will impact system 3 so as to guarantee it evolves into the state $|\psi\rangle$. Importantly, while systems 1 and 2 need to be in proximity to one another to be entangled, system 3 never needs to come into contact with system 1 and can be any distance away – this is how entanglement allows the teleportation of states between systems which are separated by arbitrarily large distances. For concreteness,

$$|\Psi_{\text{init}}\rangle = \frac{1}{\sqrt{2}}\,|\psi\rangle \otimes (|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\alpha(|000\rangle + |011\rangle) + \beta(|100\rangle + |101\rangle). \tag{94}$$

Applying a CNOT gate on qubits 1 and 2, followed by a projective measurement $\{M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|\}$, almost sets qubit 3 (here labelled $|\psi_3\rangle$) to be $|\psi_3\rangle = |\psi\rangle$. Specifically, we end up with the final state that depends on the values of qubits 1 and 2. If they are projected into $|00\rangle$, then

$$|\Psi_{\text{final}}\rangle = |00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) = |00\rangle \otimes |\psi\rangle . \tag{95}$$

In the instances where qubits 1 and 2 are projected into $|01\rangle$, $|10\rangle$ or $|11\rangle$, then a *known* single qubit gate can rotate $|\psi_3\rangle \rightarrow |\psi\rangle$. This is one example of how entanglement can be used up as a resource (i.e. destroyed through measurement) to perform quantum gates and protocols such as teleportation.

A.3 Quantum error correction

While a detailed account of quantum error correction is not included in this report [Gottesman, 2010], it should be noted that schemes exist to correct errors in quantum information.

As an example, $|0\rangle$ to $|1\rangle$ bit flip errors are often protected by replacing quantum states with logical qubits, $|0\rangle \rightarrow |000\rangle$ and $|1\rangle \rightarrow |111\rangle$. Although the number of qubits required for these schemes increases, if it is assumed that the error rates are low, measurements can be performed to correct the bit flip. More elaborate codes exist, which preserve resources and correct different kinds of errors.

If qubits can be generated faithfully and error rates are low enough, error correction schemes can lead to so–called 'fault tolerance', where protection from errors on quantum information is assured.

B Measures of the communication rate through quantum channels

In classical Shannon theory, the quantification of information and its transmission through noisy channels is well understood, and given by the entropy and channel capacity, respectively. As we have seen in the previous section, quantum Shannon theory lends itself to a much larger variety of scenarios, which each require different quantifications. In this section we begin by briefly reviewing the measures of classical information before showing how these are generalised to the various quantum cases. We will use the standard notations presented in [Wilde, 2013], in which further information on these quantifications can be found.

B.1 Communication rate of classical information

In this subsection, we review the quantification of the classical capacity of a classical communication channel, starting with the definition of entropy.

Entropy Consider an experiment with a list of possible (classical) outcomes x of a random variable X, which each occur with probability $p(x)$. Classical Shannon theory tell us that the expected amount of information gained from the result of the experiment is given by the *entropy*

$$H(X) = -\sum_x p(x) \log\, p(x)\,, \tag{96}$$

which is given in units of bits (here we take the logarithm to be base 2). For example, a fair coin has the probability of each of heads or tails equal to ½, giving an entropy of H=-0.5log0.5-0.5log0.5=1 bit.

Mutual information When information is transmitted through a noisy communication channel, then in addition to the randomness inherent in the choice of message (as quantified by the probability distribution $\{p(x)\}$), the errors occurring in the channel induce a second level of randomness. Alice encodes her message in a set of symbols $\{x\}$, which are instances of the random variable X, each sent with probability $p(x)$. Now, the possible outcomes Bob can receive are given by a set of symbols $\{y\}$, which are instances of the random variable Y, and correspond directly to the $\{x\}$. However, due to errors in transmission, Bob cannot decode the message directly with knowledge only of the sending probabilities $p(x)$. Instead, he needs to consider the conditional probabilities $p(x|y)$, which correspond to the probability that Alice actually sent x given that Bob received y. The probabilities $p(x|y)$ fully characterise the noisy channel; we assume that it is possible for the communicating parties to obtain knowledge of this distribution. Mathematically, the amount of transmitted information that is error free is quantified by the *mutual information*:

$$I(X;Y) = \sum_x \sum_y p(x,y) \log \frac{p(x|y)}{p(x)} = H(X) - H\left(X|Y\right). \tag{97}$$

Channel capacity The fundamental limit on how much information can be transmitted through a noisy channel $\mathcal{N}$ is given by the *channel capacity* $C(\mathcal{N})$, defined as the maximum number of bits that can be transmitted through the channel per use of the channel. One of the most important results in classical Shannon theory is the analytical expression for the channel capacity. In technical terms, the channel capacity is equal to the maximum of the *mutual information* of the channel $\mathcal{N}$ over all possible choices of sending probabilities [Shannon, 1948]:

$$C(\mathcal{N}) = \max_{\{p(x)\}} I(X;Y)\,. \tag{98}$$

B.2 Communication rate of classical information through quantum channels

In this subsection, we quantify the classical capacity of a quantum channel, starting with a quantum notion of entropy. This corresponds to the communication scenario described in

§3.2.1. In order to understand the definition of classical capacity, we start by defining the quantum entropy, which enables the definition of the conditional quantum entropy, followed by the quantum mutual information, and finally the Holevo information.

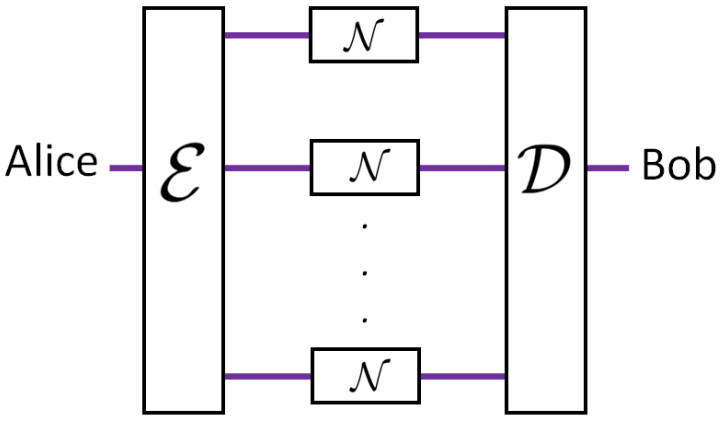

Figure 18: Communication of classical information (purple) from Alice to Bob, over multiple uses of the channel $\mathcal{N}$. $\mathcal{E}$ and $\mathcal{D}$ are the encoding and decoding operations performed by Alice and Bob, respectively, which can each be a global operation over all the channel uses.

Quantum entropy The entropy of a classical system corresponded to how much uncertainty there was in obtaining one of the possible outcomes. If we are sure what outcome is to come, then the entropy is zero; if all outcomes are equiprobable then the entropy is maximal. In the quantum case, a definition of entropy will have to capture both the classical uncertainty associated with Alice's choice of message, as well as the quantum uncertainty arising from the possible choices of measurement basis (e.g. in the case of a single photon, one could choose the basis $\{|H\rangle, |V\rangle\}$ corresponding to horizontal and vertical polarisation, or $\{|L\rangle, |R\rangle\}$, corresponding to left-handed circular and right-handed circular polarisation, cf. §2.1.3).

This can be done by replacing the probability distribution of Alice's preparation in the classical case by the density matrix of Alice's preparation – which, recall, captures both the classical and quantum types of uncertainty: The *quantum entropy*, also known as the *von Neumann entropy*, of a state ρ_A is given by:

$$H(A)_\rho := -\operatorname{Tr}\{\rho_A \log \rho_A\} \tag{99}$$

Operationally, suppose Alice produces states $|\psi_x\rangle$ in her lab with some probability distribution p_x. Then from Bob's point of view, before Alice sends him the state, the expected density matrix of the state is $\rho_A = \sum_x p_x |\psi_x\rangle \langle\psi_x|$. Now, if the states $\{|\psi_x\rangle\}$ form an orthonormal basis (corresponding to distinct classical choices), then a direct calculation reveals that we recover the classical entropy of the probability distribution $\{p_x\}$.

Conditional quantum entropy In order to define the quantum analogue to the mutual information, we first need a definition of conditional quantum entropy. This turns out to be a non-trivial task, as there is no direct analogue of conditional probabilities in the quantum case. The following definition is chosen [Wilde, 2013]: The *conditional quantum entropy* of the joint state ρ_{AB} of Alice and Bob's composite system AB is

$$H(A|B)_\rho := H(AB)_\rho - H(B)_\rho \tag{100}$$

where $\rho_B := \mathrm{Tr}_A\, \rho_{AB}$ is the marginal state as seen by Bob. (Here, Tr_A is the partial trace over subsystem A only.)

Counterintuitively, the conditional quantum entropy can be negative, illustrating one of the most important differences between the classical and quantum worlds. For example, consider the maximally entangled Bell state between Alice and Bob $|\Phi^+\rangle := (|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle)/\sqrt{2}$. $H(AB) = 0$, but the marginal state as seen by Bob is $\rho_B = \mathrm{Tr}_A\, |\Phi^+\rangle\langle\Phi^+| = I/2$, i.e. the maximally mixed state, which has a quantum entropy $H(B)_\rho = 1$, leading to $H(A|B)_\rho = -1$. Operationally, the negative conditional quantum entropy can be understood as quantifying the fact that we can know more about an entangled state as a whole than about any of its individual components.

Quantum mutual information The *quantum mutual information* can now be defined in complete analogy with the classical case:

$$I(A;B)_\rho := H(A)_\rho - H(A|B)_\rho, \tag{101}$$

or equivalently, $I(A;B)_\rho = H(A)_\rho + H(B)_\rho - H(AB)_\rho$. As in the classical case, the quantum mutual information describes the amount of classical correlations between two systems.

The most relevant communication scenario where this is useful is in the case of classical communication between two parties. Consider the scenario where Alice sends classical information through a noisy channel $\mathcal{N}$ to Bob. Alice prepares the states ρ_A^x which can be input into the channel, each with probability $p(x)$, and keeps a copy of the index of her chosen state in a classical register X with states $\{|x\rangle\}$. The expected density matrix of her prepared state is then

$$\rho_{XA} = \sum_x p(x)\, |x\rangle\langle x|_X \otimes \rho_A^x. \tag{102}$$

Now if she sends the state of the A system over to Bob via a quantum channel $\mathcal{N}_{A\to B}$ (after which we call it system B), then the joint state of Bob's received system B with Alice's remaining classical register X is

$$\rho_{XB} = \sum_x p(x)\, |x\rangle\langle x|_X \otimes \mathcal{N}_{A\to B}(\rho_A^x). \tag{103}$$

The quantum mutual information $I(X;B)_\rho$ of this state gives a measure of the classical information that Alice was able to transmit to Bob.

Holevo information of a quantum channel The fundamental question here, just as in the case of classical channels, is: what is the maximum amount of information that can be sent through a given quantum channel $\mathcal{N}$. If the input states to each use of the channel are not allowed to be entangled (as in the classical case), then the maximum number of bits that can be sent through a channel $\mathcal{N}$ per use of the channel is given by the *Holevo information*, (defined analogously to the classical capacity of a classical channel):

$$\chi(\mathcal{N}) := \max_{\rho_{XA}} I(X;B)_\rho, \tag{104}$$

where the maximisation is over all possible states of the form of eq. (102) and $I(X;B)$ is the quantum mutual information, both defined shortly.

Classical capacity of a quantum channel Yet, the Holevo information is not the ultimate limit of classical information transfer through quantum channels. Crucially, the Holevo information is non-additive, meaning that $k\chi(\mathcal{N}) \leq \chi(\mathcal{N}^{\otimes k})$. That is, the Holevo information of k parallel uses of $\mathcal{N}$ can be larger than k times the Holevo information of $\mathcal{N}$ itself. In particular, the RHS can be made larger than the LHS for certain quantum channels, when successive input states are entangled. This leads to the following expression for the *classical capacity of a quantum channel* (Holevo–Schumacher–Westmoreland Theorem):

$$C_{\mathrm{C}}(\mathcal{N}) = \lim_{k\to\infty} \frac{1}{k}\chi(\mathcal{N}^{\otimes k}), \tag{105}$$

where $\chi(\mathcal{N}^{\otimes k})$ is the Holevo information of k parallel copies of $\mathcal{N}$ [Holevo, 1998, Schumacher and Westmoreland, 1997].

In general, the classical capacity of a quantum channel is intractable to calculate, as it involves the regularisation over infinitely many copies of the channel. In practice, the Holevo information is often a useful lower bound.

Example: depolarising error As an example of a channel for which one might want to communicate classical information, consider the depolarising channel introduced in §3.3.2. To illustrate the measures of information described above, consider the completely depolarising channel, i.e. a depolarising channel where the input state is converted to a maximally mixed state with probability $p = 1$. This means that every possible output state $\mathcal{N}_{A\to B}(\rho_A^x)$ in the expression for the Holevo information (103) is independent of the classical register x, so that the quantum mutual information must always be zero. Therefore, both the Holevo information and the classical capacity of the completely depolarising channel are zero. A general depolarising channel with an error probability $0 < 1 < p$ will have a non-zero Holevo information. It has been shown that the Holevo information of the depolarising channel is additive (i.e.

does not exhibit superadditivity), and therefore the classical capacity is equal to the Holevo information [King, 2003]. The full expression is given in §3.3.

B.3 Communication rate of classical information through quantum channels with the assistance of shared entanglement

In this subsection, we quantify the entanglement-assisted classical capacity of a quantum channel. This corresponds to the communication scenario described in §3.2.2.

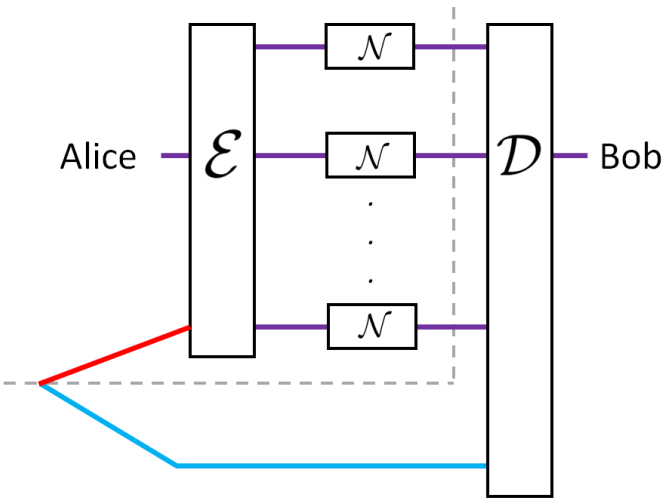

Figure 19: Communication of classical information (purple) from Alice to Bob, over multiple uses of the channel $\mathcal{N}$, with the assistance of an unlimited amount of entanglement shared between Alice and Bob (red and blue lines). $\mathcal{E}$ and $\mathcal{D}$ are the encoding and decoding operations performed by Alice and Bob, respectively, which can each be a global operation over all the channel uses, and can also make use of each party's half of the entangled state. The partition between Alice and Bob is given by the dashed grey line; note that Bob has access to the blue half of the entangled state from the start – it is not sent to him has part of the protocol – hence the shape of the partition.

Entanglement-assisted classical capacity of a quantum channel Another way in which quantum physics can help with the transmission of classical information is when the sender and receiver share entangled states prior to communicating. In this case we can ask: what is the maximum number of bits that can be transmitted through the channel per channel use, in the asymptotic limit of infinitely many channel uses, in the presence of an unlimited amount of shared entangled states between the sender and receiver? The answer is defined by the *entanglement-assisted classical capacity*, which is given by (Bennett–Shor–Smolin–Thapliyal Theorem) [Bennett et al., 1999]

$$C_{\mathrm{EA}}(\mathcal{N}) = I(\mathcal{N}), \tag{106}$$

where $I(\mathcal{N})$ is the quantum mutual information of the channel $\mathcal{N}$. Similarly to the previous examples, the quantum mutual information of a general quantum channel $\mathcal{N}$ is given by $I(\mathcal{N}) := \max_{\phi_{AA'}} I(A,B)_\rho$, where is $\phi_{AA'}$ is any bipartite pure state and $\rho := \mathcal{N}_{A'\to B}(\phi_{AA'})$.

An example of a protocol using this scenario is superdense coding, discussed in §5.3. In this case, the channel $\mathcal{N}$ is assumed to be noiseless (i.e. the identity channel), in which case $I(A,B)_\rho$ is just the quantum mutual information of the maximally entangled state, which is 2. In contrast, the classical capacity of the identity channel is 1, showing that entanglement can double the capacity.

B.4 Communication rate of private classical information through quantum channels

In this subsection, we quantify the private classical capacity of a quantum channel. This corresponds to the communication scenario described in §3.2.3.

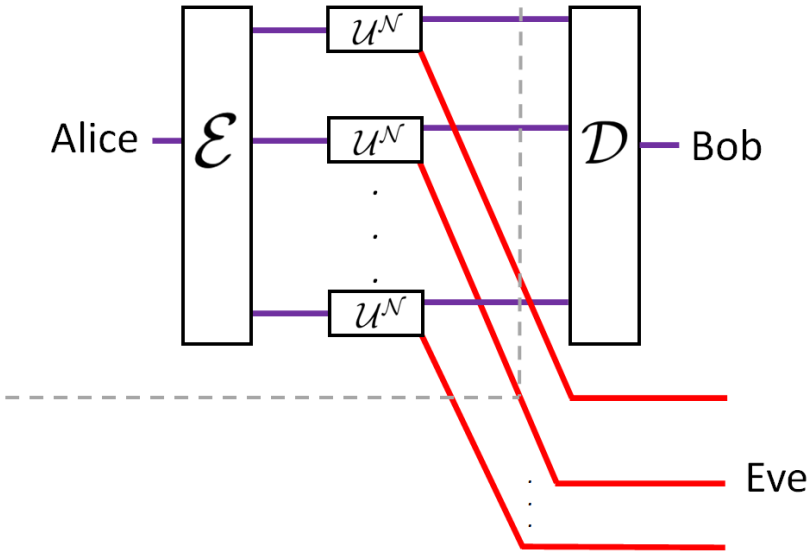

Figure 20: Communication of private classical information (purple) from Alice to Bob, over multiple uses of the channel $\mathcal{N}$, taking into account the full unitary description of noise and corresponding leakage into the environment $\mathcal{U}^{\mathcal{N}}$, which can be intercepted (red) by Eve. $\mathcal{E}$ and $\mathcal{D}$ are the encoding and decoding operations performed by Alice and Bob, respectively, which can each be a global operation over all the channel uses. The partitions between Alice, Bob, and Eve are given by the dashed grey lines.

When information is transmitted through a noisy channel from Alice to Bob, the evolution of the quantum state carrying the information is described by a quantum channel. Physically, however, a quantum channel is only the description of the noisy evolution as seen from the perspective of Alice and Bob, whilst in reality the fundamental description of any quantum

evolution is given by unitary dynamics (§2.2.3). That is, for any given quantum channel, the full description of the physical scenario is given by a unitary operator that includes all the interactions with the environment which induce the noise. When information is lost due to noise, it means that the information has leaked out into the environment. A complete unitary description of the physical scenario conserves information: the information initially sent by Alice but not received by Bob can be retrieved from the environment by an eavesdropper Eve. Remarkably, the amount of information accessible to Eve via any unitary description of the whole scenario can be quantified by knowing only the input-output description of the quantum channel.

Yet, due to the no-cloning theorem, only the information not received by Bob can be obtained by Alice. This means that for any given channel, the maximum amount of information receivable by Bob but inaccessible to Eve can be quantified.

Private classical capacity of a quantum channel The maximum number of bits that can be transmitted through the channel from the sender to the receiver, per channel use, in the asymptotic limit of infinitely many uses, such that the transmitted bits are inaccessible to anyone else, is given by the private classical capacity of the channel. This communication task is depicted in Figure 20.

The *private classical capacity* is given by the following expression (Devetak–Cai–Winter–Yeung Theorem):

$$C_{\mathrm{P}}(\mathcal{N}) = \lim_{k\to\infty} \frac{1}{k} P(\mathcal{N}^{\otimes k}), \tag{107}$$

where $P(\mathcal{N})$ is the private information of channel $\mathcal{N}$, defined by

$$P(\mathcal{N}) := \max_{\rho} [I(X;B)_\sigma - I(X;E)_\sigma], \tag{108}$$

where the maximisation is over all classical-quantum states ρ_{XA} of he form of eq. (102) which Alice can input into the channel. $I(X;B)_\sigma$ is the quantum mutual information between Alice's classical register X and Bob's received system B; $I(X;E)_\sigma$ is the quantum mutual information between Alice's classical register X and any potential eavesdropper Eve's received system E [Wilde, 2013]. This is quantified by σ, the joint state of Alice, Bob and Eve, resulting from the action of the channel $\mathcal{N}$ and taking into account all possible ways in which information could have been lost from the channel into the environment. (Formally, $\sigma_{XBE} := \mathcal{U}^{\mathcal{N}}_{A\to BE}(\rho_{XA})$, where $U^{\mathcal{N}}_{A\to BE}$ is an 'isometric extension' of $\mathcal{N}_{A\to B}$, that is, the unitary evolution that takes into account both the information transfer via the channel from Alice to Bob as well as any leakage into the environment E which can be intercepted by Eve.)

B.5 Communication rate of quantum information through quantum channels

In this subsection, we quantify the quantum capacity of a quantum channel, starting with the definition of the coherent information of a quantum state, and then the coherent information of a quantum channel. This corresponds to the communication scenario described in §3.2.4.

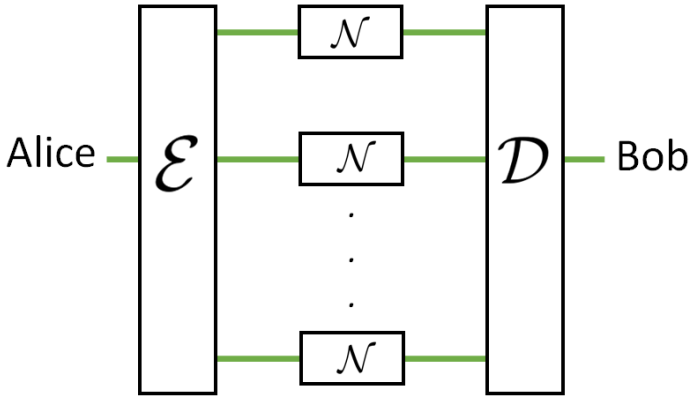

Figure 21: Communication of quantum information (green) from Alice to Bob, over multiple uses of the channel $\mathcal{N}$. $\mathcal{E}$ and $\mathcal{D}$ are the encoding and decoding operations performed by Alice and Bob, respectively, which can each be a global operation over all the channel uses.

Coherent information A standard measure of the amount of quantum correlations between two systems is given by the *coherent information*:

$$I(A\rangle B)_\rho := H(B)_\rho - H(AB)_\rho, \tag{109}$$

which, interestingly, is equal to the negative of the conditional quantum entropy. This equivalence can be understood from the example above of the maximally entangled state which has maximal negative conditional quantum entropy. The essence of establishing quantum correlations is establishing entanglement, so it makes sense that a measure of information which is maximised for a maximally entangled state corresponds to a quantification of quantum correlations.

Coherent information of a quantum channel The extent to which a quantum channel can preserve quantum correlations in the presence of noise is quantified by the coherent information of a quantum channel, defined similarly to the Holevo information in the case of classical information. Consider a pure bipartite state $\phi_{AA'}$ in Alice's possession, where she sends the A' system to Bob through a channel $\mathcal{N}A' \to B$. If the initial state $\phi_{AA'}$ is entangled, then we

would want the final state $\rho_{AB} = \mathcal{N}_{A' \to B}(\phi_{AA'})$ to preserve this entanglement. The *coherent information of a quantum channel* is defined as

$$Q(\mathcal{N}) := \max_{\phi_{AA'}} I(A\rangle B)_\rho, \tag{110}$$

where the maximisation is with respect to all pure states $\phi_{AA'}$. Just like the Holevo information of a quantum channel, the coherent information of a quantum channel is not in general additive, meaning that $kQ(\mathcal{N}) \leq Q(\mathcal{N}^{\otimes k})$.

Quantum capacity of a quantum channel The quantum capacity of a quantum channel is the maximum number of qubits that can be transmitted through the channel per channel use, in the asymptotic limit of infinitely many channel uses. This is the fully quantum analogue of the channel capacity in classical Shannon theory. The *quantum capacity of a quantum channel* is given by (quantum capacity theorem):

$$C_{\mathrm{Q}}(\mathcal{N}) = \lim_{k \to \infty} \frac{1}{k} Q(\mathcal{N}^{\otimes k}). \tag{111}$$

where $Q(\mathcal{N})$ is the coherent information of channel $\mathcal{N}$. (The quantum capacity theorem is a result of the work of many different authors; a standard reference is the textbook by Wilde [Wilde, 2013].)

The quantum capacity possesses a striking property: it is possible that two quantum channels, each with zero quantum capacity when used individually, have a non-zero quantum capacity when combined in parallel – a phenomenon known as superactivation [Smith and Yard, 2008].

Example: dephasing error As an example of a channel with zero quantum capacity but unit classical capacity, consider the qubit completely dephasing channel (§3.3.3). To see what it does to the coherent information and quantum capacity, note that if one half of an entangled state is sent through a completely dephasing channel, then the entanglement is completely destroyed. This means that the coherent information is zero, and therefore also the quantum capacity. On the other hand, the computational basis states $|0\rangle$ and $|1\rangle$ can be transmitted error-free through the channel, meaning that the classical capacity of a completely dephasing channel is 1 bit per channel use.

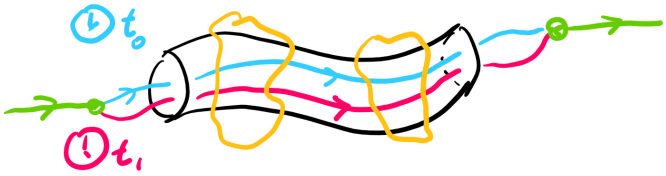

Figure 22: A single particle sent through a transmission line in a superposition of two different times t_0 (blue) and t_1 (magenta). The particle experiences errors (yellow regions) along the way, which are generally correlated between the two times.

C Further examples of the quantum configuration of transmission lines

C.1 Quantum control over the time of transmission

In many communication scenarios, the errors occurring in consecutive uses of the same transmission line are correlated. For example, a photon travelling through an optical fibre will be subject to random changes in its polarisation, and since these changes happen over a finite timescale, two photons travelling within this timescale will experience approximately the same errors. Correlated errors present both a threat and an opportunity for error correction. On the one hand, the correlations in errors undermine the effectiveness of standard error correcting codes. On the other hand, knowledge of these correlations can be used to construct more effective codes to transmit information over multiple particles [Macchiavello and Palma, 2002].

Classically, the use of multiple particles in order to probe these correlations is essential. However, in the quantum case, recent work has shown that the correlations can be probed and even used for communication enhancements, with only a single quantum particle, if the particle is sent at the superposition of different times [Kristjánsson et al., 2020]. In practice, this means that the time at which the photon is sent is treated as a quantum degree of freedom (i.e. the time bin degree of freedom – see §4.2.1), with the single particle being sent simultaneously at time t_0 and t_1, in a quantum superposition of the classical basis states $|t_0\rangle$ and $|t_1\rangle$, corresponding to definite times. This can, for example, be achieved using a variable beam splitter and a fibre loop, as decribed in 4.2.1; a recent implementation can be found in [Ghafari et al., 2019].

The mathematical description of this scenario is similar to that of the quantum control over trajectories, so will be omitted here for brevity.

The use of correlated quantum channels at a superposition of times can yield even stronger advantages over standard quantum Shannon theory than using independent quantum channels in a superposition of trajectories. As an example, consider again a transmission line which acts as the completely depolarising channel at every time step. Physically, one way in which the completely depolarising channel occurs in practice is when the particle undergoes one of the

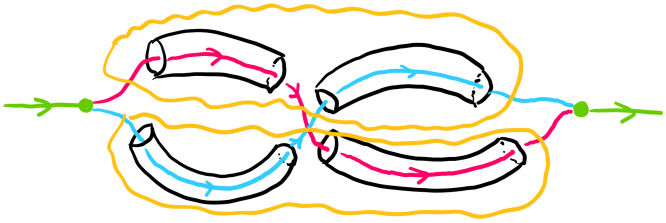

Figure 23: The trajectories (blue and magenta, respectively) of single particle sent through two different regions (yellow) in a superposition of orders.

four processes I, X, Y, Z at random with equal probability. Here, I is the identity operation, i.e. no error, and X, Y, Z are the Pauli operations (§2.1.3). If the particular choice of which one of the four noisy processes occurs at a given time t depends on the random choice of noisy process at time $t-1$, then the errors at consecutive time steps are correlated.

The most extreme communication enhancement occurs when the correlations are described by the permutations $X \to Y, Y \to X, I \to Z, Z \to I$. In this particular case (assuming a specific form of some additional parameters of the transmission line), it is possible to obtain a perfect classical communication channel of *1 bit per channel* use from Alice to Bob [Kristjánsson et al., 2020]. As in the case of superposition of trajectories, Alice encodes her information in the polarisation of the photon, whilst the time of transmission is in a fixed equal superposition of two distinct times. Then, Bob measures the time at which he receives the photon in the same superposition basis, enabling him to recover the information encoded by Alice. Here, we see that using correlated channels enables two complete white noise transmission lines to be converted into a perfect communication line – a phenomenon not achievable with the superposition of independent channels.

C.2 Quantum control over the order of transmission lines

In classical communication networks, transmission lines are placed in some configuration between the communication parties. For example, if we have two transmission lines $\mathcal{A}$ and $\mathcal{B}$, that can be used to connect the sender to the receiver via an intermediate node, then either $\mathcal{A}$ can be placed before $\mathcal{B}$ or $\mathcal{B}$ before $\mathcal{A}$. Using the full power of quantum theory, however, it is possible to create a third configuration from the two orders above: it is possible to connect the transmission lines in an indefinite order between the sender and receiver [Chiribella et al., 2009, Chiribella et al., 2013]. More precisely, it is possible to construct a quantum superposition of the two alternative orders AB and BA, if the order itself is treated as a quantum state.

In optical quantum communication networks, the superposition of orders of transmission lines can be constructed when two regions of space, R_A and R_B are available for transmission, and each of the two regions causes incoming photons to undergo time-correlated noise. Then, a particle can be sent through R_A (at time t_0) followed by R_B (at time t_1), and, R_B (at time t_0) followed by R_A (at time t_1), in a quantum superposition. If the correlations in noise in each of the two regions are such that whatever noisy process occurs at times t_0 also occurs

at t_1 (assuming the time difference $t_1 - t_0$ is short), then we have effectively achieved a superposition of the orders of the communication channels corresponding to the two regions.

The superposition of orders of two noisy transmission lines exhibits various communication advantages over standard quantum Shannon theory, including effect not achievable using the superposition of trajectories alone [Ebler et al., 2018, Salek et al., 2018, Chiribella et al., 2021, Goswami et al., 2018, Procopio et al., 2019, Procopio et al., 2020, Chiribella et al., 2020], some of which have been experimentally demonstrated [Goswami et al., 2018, Guo et al., 2020, Rubino et al., 2021]. In particular, as an extreme example, consider the case where both regions correspond to a completely dephasing channel (zero quantum capacity) when used at a definite time. In this case, the superposition of orders can generate a perfect quantum communication channel with quantum capacity of *1 qubit per channel use* [Chiribella et al., 2021]. (Recall, for the superposition of independent channels in §3.6.1, this was only possible with 25% probability).