1
Introduction to Quantum Information Processing

Quantum information is a relatively young area of interdisciplinary research. One of its main goals is, from a more conceptual point of view, to combine the principles of quantum physics with those of information theory. Information is physical is one of the key messages, and, on a fundamental level, it is quantum physical. Apart from its conceptual importance, however, quantum information may also lead to real-world applications for communication (quantum communication) and computation (quantum computation) by exploiting quantum properties such as the superposition principle and entanglement. In recent years, especially entanglement turned out to play the most prominent role, representing a universal resource for both quantum computation and quantum communication. More precisely, multipartite entangled, so-called cluster states are a sufficient resource for universal, measurement-based quantum computation [1]. Further, the sequential distribution of many copies of entangled states in a quantum repeater allow for extending quantum communication to large distances, even when the physical quantum channel is imperfect such as a lossy, optical fiber [2, 3].

In this introductory chapter, we shall give a brief, certainly incomplete, and in some sense biased overview of quantum information. It will be incomplete, as the focus of this book is on optical quantum information protocols, and their experimental realizations, including many experiment-oriented details otherwise missing in textbooks on quantum information. Regarding the more abstract, mathematical foundations of quantum information, there are various excellent sources already existing [4–8].

Nonetheless, we do attempt to introduce some selected topics of quantum information theory, which then serve as the conceptual footing for our detailed descriptions of the most recent quantum information experiments. In this sense, on the one hand, we are biased concerning the chosen topics. On the other hand, as our goal is to advertise a rather new concept for the realization of quantum information protocols, namely, the combination of notions and techniques from two complementary approaches, our presentation of the basics of quantum information should also provide a new perspective on quantum information. The two complementary approaches are the two most commonly used encodings of quantum information: the one based upon discrete two-level systems (so-called qubits), certainly by far the most popular and well-known approach, in analogy to classi-

Quantum Teleportation and Entanglement. Akira Furusawa, Peter van Loock
Copyright © 2011 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim
ISBN: 978-3-527-40930-3

cal digital encodings; the other approach relies on infinite-dimensional quantum systems, especially quantized harmonic oscillators (so-called qumodes), more reminiscent of classical analog encodings.

There are also approaches in between based on elementary systems that live in more than two, but still finite dimensions. Such discrete multi-level systems share many of their most distinct features with those of simple qubit systems. In fact, we may simulate any d-level system (so-called qudit) by a set of $\log_2 d$ qubits. Therefore, one may expect to obtain qualitatively new features only when the limit $d \to \infty$ is taken. Schemes based on qubit and qudit encodings are commonly referred to as discrete-variable (DV) approaches, whereas those exploiting infinite-dimensional systems and the possibility of preparing and measuring quantum information in terms of variables with a continuous spectrum are called continuous-variable (CV) schemes. Many fundamental results of quantum information theory, however, would not even depend on a particular encoding or dimensionality. These results based on fundamental elements of quantum theory such as linearity stay solid even when the infinite-dimensional limit is taken.

Similar to a classical, digital/analog hybrid computer, one may also consider utilizing discrete and continuous degrees of freedom at the same time for encoding, logic gates, or measurements. Later, when we start discussing optical implementations of quantum information protocols in Chapter 2, we can give the motivation as to why such a hybrid approach would be useful for processing quantum information. The purpose of the present chapter is solely conceptual and independent of potential implementations. We shall introduce some basic results and notions of quantum information theory, and, in particular, apply these to both DV qubit and CV qumode systems.

Starting with a short motivation for the interest in quantum information theory in Section 1.1, we discuss the preparation and representation of quantum information in the form of quantum states and observables (Section 1.2), its manipulation using unitary gates and evolution (Section 1.3), and its behavior under non-unitary evolution in the form of quantum channels and measurements (Section 1.4). The latter scenario is very important, as an initialized quantum information carrier would typically be subject to unwanted interactions with its environment, and such a pure-into-mixed-state evolution is described by a channel map (Section 1.4.1). Whenever the environment is replaced by an auxiliary system that can be measured, information about the original quantum system may be obtained, as we discuss in Section 1.4.2.

Before concluding this chapter in Section 1.10 with a discussion of some non-optical experimental realizations of quantum information processing, we briefly introduce some basic notions, resources, subroutines, and full-scale applications such as entanglement (Section 1.5), quantum teleportation (Section 1.6), quantum communication (Section 1.7), quantum computation (Section 1.8), and quantum error correction (Section 1.9). Since the remainder of this book is intended to describe and illustrate many of these protocols and applications, we shall postpone such more detailed discussions until the respective chapters regarding optical implementations.

1.1 Why Quantum Information?

Quantum computers are designed to process information units which are no longer just abstract mathematical entities according to Shannon's theory, but rather truly physical objects, adequately described by one of the two[1] most fundamental physical theories – quantum mechanics.

Classical information is typically encoded in digital form. A single basic information unit, a bit, contains the information whether a "zero" or a "one" has been chosen between only those two options, for example, depending on the electric current in a computer wire exceeding a certain value or not. Quantum information is encoded in quantum mechanical superpositions, most prominently, an arbitrary superposition of "zero" and "one", called a "qubit".[2] Because there is an infinite number of possible superposition states, each giving the "zero" and the "one" particular weights within a continuous range, even just a single qubit requires, in principle, an infinite amount of information to describe it.

We also know that classical information is not necessarily encoded in bits. Bits may be tailor-made for handling by a computer. However, when we perform calculations ourselves, we prefer the decimal to the binary system. In the decimal system, a single digit informs us about a particular choice between ten discrete options, not just two as in the binary system. Similarly, quantum information may also be encoded into higher-dimensional systems instead of those qubit states defined in a two-dimensional Hilbert space. By pushing the limits and extending classical analog encoding to the quantum realm, quantum observables with a continuous spectrum may also serve as an infinite-dimensional basis for encoding and processing quantum information. In this book, we shall attempt to use both the discrete and the continuous approaches in order to formulate quantum information protocols, to conceptually understand their meaning and significance, and to recast them into a form most accessible to experimental implementations. We will try to convey some answers as to why quantum information is such a fascinating field that stimulates interdisciplinary research among physicists, mathematicians, computer scientists, and others.

There is one answer we can offer in this introductory chapter straight away. In most research areas of physics, normally a physicist has to make a choice. If she or he is most interested in basic concepts and the most fundamental theories, she or he may acquire sufficient skills in abstract mathematical formalisms and become part of the joint effort of the physics community to fill some of the gaps in the basic physical theories. Typically, this kind of research, though of undoubted importance for the whole field of physics as such, is arbitrarily far from any real-world applications. Often, these research lines even remain completely disconnected from any potential experimental realizations which could support or falsify the corresponding theory. On the other hand, those physicists who are eager to contribute to the

[1] The other, complementary, fundamental physical theory is well known to be general relativity.

[2] The term qubit was coined by Schumacher [9].

real world by using their knowledge of fundamental physical theories would typically have to sacrifice (at least to some extent)[3] their deeper interest into those theories and concepts, as day and life times are finite.

Thus, here is one of the most attractive features of the field of quantum information: it is oriented towards both directions, namely, one that aims at a deeper understanding of fundamental concepts and theories, and, at the same time, one that may lead to new forms of communication and computation for real-world applications.[4] Obviously, as quantum information has been an interdisciplinary field from the beginning, the large diversity of quantum information scientists naturally means that some of them would be mainly devoted to abstract, mathematical models, whereas others would spend most of their time attempting to bridge the gaps between theoretical proposals, experimental proof-of-principle demonstrations, and, possibly, real-world applications. However, and this is maybe one of the most remarkable aspects of quantum information, new fundamental concepts and insights may even emerge when the actual research effort is less ambitious and mostly oriented towards potential applications. In fact, even without sophisticated extensions of the existing mathematical formalisms, within the standard framework of quantum mechanics, deep insights may be gained. A nice example of this is the famous no-cloning theorem [14, 15] which is, historically, probably the first fundamental law of quantum information.[5]

The no-cloning theorem states that quantum information encoded in an arbitrary, potentially unknown quantum state cannot be copied with perfect accuracy. This theorem has no classical counterpart because no fundamental principle prevents us from making arbitrarily many copies of classical information. The no-cloning theorem was one of the first results on the more general concepts of quantum theory that had the flavor of today's quantum information theory (see Figure 1.1). Though only based upon the linearity of quantum mechanics, no-cloning is of fundamental importance because it is a necessary precondition for physical laws as fundamental as no-signaling (i.e., the impossibility of superluminal communication) and the Heisenberg uncertainty relation.

[3] A famous exception, of course, is Albert Einstein who dealt with fridges during his working hours in a patent office and discovered general relativity during his spare time.

[4] Very recent examples for these two complementary directions are, on the one hand, the emerging subfield of relativistic quantum information that is intended to provide new insights into more complete theories connecting quantum mechanics with relativity [10, 11]; and, on the other hand, the recent demonstration of a quantum key distribution network in Vienna [12, 13].

[5] There is a fascinating anecdote related to the discovery of no-cloning in 1982. The theorem was inspired by a proposal for a "superluminal communicator", the so-called FLASH (an acronym for First Laser-Amplified Superluminal Hookup) [16]. The flaw in this proposal and the non-existence of such a device was realized by both referees: Asher Peres, who nonetheless accepted the paper in order to stimulate further research into this matter, and GianCarlo Ghirardi, who even gave a no-cloning-based proof for the incorrectness of the scheme in his report. Eventually, the issue was settled through the published works by Dieks, Wootters, and Zurek [14, 15], proving that *any* such device would be unphysical.

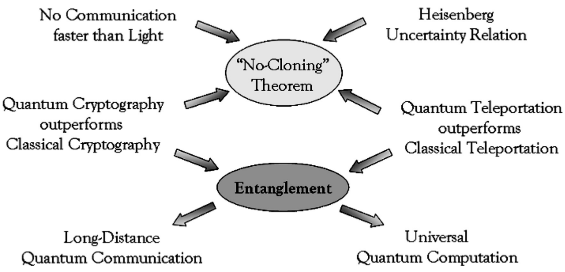
No Communication faster than Light
Heisenberg Uncertainty Relation
"No-Cloning" Theorem
Quantum Cryptography outperforms Classical Cryptography
Quantum Teleportation outperforms Classical Teleportation
Entanglement
Long-Distance Quantum Communication
Universal Quantum Computation

Figure 1.1 A summary of concepts and applications linked to or originating from quantum information. The upper part is devoted to fundamental physical laws, while the middle and lower parts refer to elementary quantum protocols and the ultimate full-scale quantum applications, respectively.

At the center of quantum information is the notion of entanglement, a necessary resource for elementary quantum protocols such as quantum teleportation [17] (the reliable transfer of quantum information using shared entanglement and classical communication) and quantum key distribution [18] (the secure transmission of classical information using quantum communication);[6] entanglement has also been shown to be a sufficient resource for the ultimate applications, long-distance quantum communication [2] and universal quantum computation [1]. Missing in Figure 1.1 are important subroutines for quantum error correction [5, 21] in order to distribute or reliably store entanglement; in quantum communication, such a quantum error correction may be probabilistic (so-called entanglement distillation [22]), while for quantum computation, we need to measure and manipulate entangled states fault-tolerantly in a deterministic fashion [5].

Without no-cloning, the following scenario appears to be possible [16]. Two parties, "Alice" (subscript A) and "Bob" (subscript B), sharing a maximally entangled two-qubit state,[7]

$$\frac{1}{\sqrt{2}}\left(|0\rangle_{\rm A}\otimes|0\rangle_{\rm B}+|1\rangle_{\rm A}\otimes|1\rangle_{\rm B}\right)=\frac{1}{\sqrt{2}}\left(|+\rangle_{\rm A}\otimes|+\rangle_{\rm B}+|-\rangle_{\rm A}\otimes|-\rangle_{\rm B}\right)\ , \tag{1.1}$$

may use their resource to communicate faster than the speed of light. The essential element for this to work would be the Einstein, Podolsky, and Rosen (EPR) [23]

[6] The importance of entanglement as a necessary precondition for secure key distribution was shown by Curty *et al.* [19]. Even though entanglement may not be physically distributed between the sender and the receiver (as in [18], as opposed to, for example, the Ekert protocol [20]), for secure communication, the measured correlations must not be consistent with classical correlations described by an unentangled state. Note that a possible eavesdropper attack is always given by approximate cloning of the quantum signals such that perfect cloning would definitely prevent secure quantum key distribution (Figure 1.1), and, in a realistic scenario, approximate cloning may as well.

[7] The following discussion requires some familiarity with basic quantum mechanical notions such as state vectors, density operators, and partial trace operations, a brief introduction of which will be given in the succeeding section.

correlations of the entangled state which are stronger than classical correlations as they are present at the same time in different, conjugate bases, $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ with $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$, corresponding to different, non-commuting observables Z and X, respectively, where $Z|k\rangle = (-1)^k|k\rangle$ and $X|\pm\rangle = \pm|\pm\rangle$ with $k = 0, 1$. Physically, each of the two bases could correspond to two orthogonal polarizations of a single photon; one basis for linear polarization and the other one for circular polarization.

Alice could now choose to measure her half of the entangled state in the basis $\{|0\rangle, |1\rangle\}$. Alternatively, she may as well project onto $\{|+\rangle, |-\rangle\}$. In the former case, Bob's half ends up in the corresponding eigenstate $|0\rangle$ or $|1\rangle$ and so would all copies that he could generate from his half. In the latter case, copies of Bob's half would all be in the corresponding state $|+\rangle$ or $|-\rangle$, and measurements in the basis $\{|0\rangle, |1\rangle\}$ would yield, on average, half of the copies in the state $|0\rangle$ and likewise half of them in the state $|1\rangle$. Therefore, the statistics of measurements on copies of Bob's half would enable him to find out which measurement basis Alice has chosen. Such a scheme could be exploited for a deterministic, superluminal transfer of binary information from Alice to Bob. However, the other crucial element here would be Bob's capability of producing many copies of the states $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ without knowing what the actual states are. This is forbidden by the no-cloning theorem.

Physically, no-cloning would become manifest in an optical implementation of the above scheme through the impossibility of amplifying Bob's photons in a noiseless fashion; spontaneous emissions would add random photons and destroy the supposed correlations. From a mathematical, more fundamental point of view, the linearity of quantum mechanics alone suffices to negate the possibility of superluminal communication using shared entanglement.

The crucial ingredient of the entanglement-assisted superluminal communication scenario above is the copying device that may be represented by an (initial) state $|\mathrm{A}\rangle$. It must be capable of copying *arbitrary* quantum states $|\psi\rangle$ as

$$|\psi\rangle|\mathrm{A}\rangle \longrightarrow |\psi\rangle|\psi\rangle|\mathrm{A}'\rangle \ . \tag{1.2}$$

The final state of the copying apparatus is described by $|\mathrm{A}'\rangle$. More accurately, the transformation should read

$$|\psi\rangle_\mathrm{a}|0\rangle_\mathrm{b}|\mathrm{A}\rangle_\mathrm{c} \longrightarrow |\psi\rangle_\mathrm{a}|\psi\rangle_\mathrm{b}|\mathrm{A}'\rangle_\mathrm{c} \ , \tag{1.3}$$

where the original input a to be cloned is described by $|\psi\rangle_\mathrm{a}$ and a second qubit b is initially in the "blank" state $|0\rangle_\mathrm{b}$. After the copying process, both qubits end up in the original quantum state $|\psi\rangle$.

Wootters and Zurek [15] (and similarly Dieks for his "multiplier" [14]) considered a device that does clone the basis states $\{|0\rangle, |1\rangle\}$ in the appropriate way according to Eq. (1.2),

$$\begin{aligned} |0\rangle|\mathrm{A}\rangle &\longrightarrow |0\rangle|0\rangle|\mathrm{A}_0\rangle \ , \\ |1\rangle|\mathrm{A}\rangle &\longrightarrow |1\rangle|1\rangle|\mathrm{A}_1\rangle \ . \end{aligned} \tag{1.4}$$

Since this transformation must be unitary[8] and linear, its application to an input in the superposition state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ leads to

$$|\psi\rangle|\mathrm{A}\rangle \longrightarrow \alpha|0\rangle|0\rangle|\mathrm{A}_0\rangle + \beta|1\rangle|1\rangle|\mathrm{A}_1\rangle \ . \tag{1.5}$$

For identical output states of the copying apparatus, $|\mathrm{A}_0\rangle = |\mathrm{A}_1\rangle$, a and b are in the pure state $\alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle$ which is not the desired output state $|\psi\rangle|\psi\rangle$. With a distinction between the apparatus states, that is, taking them to be orthonormal, $\langle \mathrm{A}_0|\mathrm{A}_0\rangle = \langle \mathrm{A}_1|\mathrm{A}_1\rangle = 1$, $\langle \mathrm{A}_0|\mathrm{A}_1\rangle = 0$, we obtain from the density operator of the whole output system (for simplicity, assuming real α and β),

$$\begin{aligned}\hat{\rho}_{\mathrm{abc}} = \alpha^2|00\mathrm{A}_0\rangle_{\mathrm{abc}}\langle 00\mathrm{A}_0| + \beta^2|11\mathrm{A}_1\rangle_{\mathrm{abc}}\langle 11\mathrm{A}_1| \\ + \alpha\beta|00\mathrm{A}_0\rangle_{\mathrm{abc}}\langle 11\mathrm{A}_1| + \alpha\beta|11\mathrm{A}_1\rangle_{\mathrm{abc}}\langle 00\mathrm{A}_0| \ ,\end{aligned} \tag{1.6}$$

the density operator of the original-copy system ab by tracing out the apparatus,

$$\mathrm{Tr}_{\mathrm{c}}\hat{\rho}_{\mathrm{abc}} = \alpha^2|00\rangle_{\mathrm{ab}}\langle 00| + \beta^2|11\rangle_{\mathrm{ab}}\langle 11| \equiv \hat{\rho}_{\mathrm{ab}} \ . \tag{1.7}$$

Finally, we can calculate the individual density operators of a and b,

$$\begin{aligned}\mathrm{Tr}_{\mathrm{b}}\hat{\rho}_{\mathrm{ab}} &= \alpha^2|0\rangle_{\mathrm{a}}\langle 0| + \beta^2|1\rangle_{\mathrm{a}}\langle 1| \equiv \hat{\rho}_{\mathrm{a}} \ , \\ \mathrm{Tr}_{\mathrm{a}}\hat{\rho}_{\mathrm{ab}} &= \alpha^2|0\rangle_{\mathrm{b}}\langle 0| + \beta^2|1\rangle_{\mathrm{b}}\langle 1| \equiv \hat{\rho}_{\mathrm{b}} \ .\end{aligned} \tag{1.8}$$

The two outgoing states are identical, but significantly different from the desired original density operator,

$$|\psi\rangle_{\mathrm{a}}\langle\psi| = \alpha^2|0\rangle_{\mathrm{a}}\langle 0| + \alpha\beta|0\rangle_{\mathrm{a}}\langle 1| + \alpha\beta|1\rangle_{\mathrm{a}}\langle 0| + \beta^2|1\rangle_{\mathrm{a}}\langle 1| \ . \tag{1.9}$$

In fact, any information about quantum coherence encoded in the off-diagonal terms of $|\psi\rangle$ is eliminated in the output states of Eq. (1.8). The degree of similarity between the actual output states and the original state, expressed by their overlap, the so-called fidelity [9],

$$F = {}_{\mathrm{a}}\langle\psi|\hat{\rho}_{\mathrm{a}}|\psi\rangle_{\mathrm{a}} = {}_{\mathrm{b}}\langle\psi|\hat{\rho}_{\mathrm{b}}|\psi\rangle_{\mathrm{b}} = \alpha^4 + \beta^4 = \alpha^4 + (1-\alpha^2)^2 \ , \tag{1.10}$$

depends on the original input state. The basis states $|0\rangle$ or $|1\rangle$ are perfectly copied with unit fidelity ($\alpha = 1$ or $\alpha = 0$), as we know from Eq. (1.4). However, coherent superpositions are copied with non-unit fidelity, where the worst result is obtained for the symmetric superposition $\alpha = 1/\sqrt{2}$ with $F = 1/2$.

Is it inevitable to obtain such a bad result when copying a symmetric superposition? Of course, only when we insist on perfectly copying certain basis states such

[8] It was pointed out by Werner [24] that the "constructive" approach here, i.e, coupling the input system with an apparatus or "ancilla" through a unitary transformation and then tracing out the ancilla, is equivalent to a general quantum cloner described by linear, completely positive trace-preserving (CPTP) maps. General quantum operations, channels, and CPTP maps as well as states represented by density operators instead of vectors in Hilbert space will be discussed in more detail in the following sections.

as $\{|0\rangle, |1\rangle\}$. A universal copying machine that "treats all input states equally well" could be considered instead. For any input state $|s\rangle = \alpha|0\rangle + \beta|1\rangle$, it would always yield the same optimal non-unit fidelity independent of α, namely, $F = 5/6$ [25]. This would correspond to the optimal, approximate, universal cloning of an unknown qubit.

Since no-cloning only depends on the linearity of quantum theory, it applies to quantum states of any dimensionality, not only to qubits. Optimal, approximate, universal cloning may then be considered for all kinds of quantum states, from DV *d*-level systems [24] to CV infinite-dimensional systems [26, 27], including extensions with certain given numbers of input and output copies.

1.2 States and Observables

A *pure* quantum state is given by a vector in Hilbert space $|\psi\rangle$, and the vector may be expanded in an arbitrary basis,

$$|\psi\rangle = \sum_m \langle m|\psi\rangle |m\rangle \ . \tag{1.11}$$

The basis is complete and orthonormal,

$$\sum_m |m\rangle\langle m| = \mathbb{1} \ , \langle m|m'\rangle = \delta_{mm'} \ . \tag{1.12}$$

The complex numbers $\langle m|\psi\rangle$ are the components of the Hilbert space vector $|\psi\rangle$. When measuring an observable $\hat{M}$, the probability for obtaining the measurement result m (a *real* eigenvalue of $\hat{M}$ with eigenstate $|m\rangle$) is determined by the size of the component of $|\psi\rangle$ in direction of $|m\rangle$,

$$p_m = \frac{|\langle m|\psi\rangle|^2}{\langle\psi|\psi\rangle} \ . \tag{1.13}$$

Here,

$$\langle\psi|\psi\rangle = \sum_m \sum_{m'} \langle\psi|m\rangle\langle m|\langle m'|\psi\rangle|m'\rangle = \sum_m |\langle m|\psi\rangle|^2 \tag{1.14}$$

ensures the proper normalization, with $\langle m|\psi\rangle^* = \langle\psi|m\rangle$. Once the measurement result m is obtained, the state vector $|\psi\rangle$ is reduced ("collapses") onto the corresponding eigenstate $|m\rangle$. The overlap $\langle\psi|\psi'\rangle$ is the scalar product of the vector space, which is obviously independent of the basis choice in Eq. (1.11). The expectation value of the observable $\hat{M}$ in the state $|\psi\rangle$ is given by (with $\langle\psi|\psi\rangle = 1$)

$$\begin{aligned}\langle\hat{M}\rangle &= \sum_m p_m m = \sum_m m\langle\psi|m\rangle\langle m|\psi\rangle \\ &= \langle\psi|\sum_m m|m\rangle\langle m|\psi\rangle = \langle\psi|\hat{M}|\psi\rangle \ .\end{aligned} \tag{1.15}$$

This equation reveals the *spectral decomposition* of the observable $\hat{M}$,

$$\hat{M} = \sum_m m|m\rangle\langle m| \,, \tag{1.16}$$

which is a Hermitian operator and so the eigenvalues m are real. Thus far, we have considered observables with a *discrete, countable* spectrum, regardless of whether the Hilbert space is finite or infinite-dimensional. In the infinite-dimensional case, an observable $\hat{X}$ may have a *continuous* spectrum. Its spectral decomposition becomes

$$\hat{X} = \int \mathrm{d}x\, x|x\rangle\langle x| \,, \tag{1.17}$$

with the continuous eigenbasis $\{|x\rangle\}$ and the real, continuous eigenvalues x.

In contrast to pure states, *mixed* states cannot be described by Hilbert space vectors, taking into account the case of incomplete knowledge about the state preparation. A mixed state is a statistical mixture of pure states given by the density operator (with $\rho_k > 0$ and $\sum_k \rho_k = 1$)

$$\hat{\rho} = \sum_k \rho_k |\psi_k\rangle\langle\psi_k| \,. \tag{1.18}$$

As opposed to the coherent superposition in Eq. (1.11), a mixed state is sometimes called an incoherent superposition. According to this definition, we find for the overall expectation value of the observable $\hat{M}$,

$$\begin{aligned}\langle\hat{M}\rangle &= \sum_k \rho_k \langle\psi_k|\hat{M}|\psi_k\rangle = \sum_m\sum_k \rho_k\langle\psi_k|\hat{M}|m\rangle\langle m|\psi_k\rangle \\ &= \sum_m \langle m|\sum_k \rho_k|\psi_k\rangle\langle\psi_k|\hat{M}|m\rangle = \mathrm{Tr}(\hat{\rho}\hat{M}) \,,\end{aligned} \tag{1.19}$$

where we have introduced the trace operation $\mathrm{Tr}(\cdots) = \sum_m \langle m|\cdots|m\rangle$ with an arbitrary basis $\{|m\rangle\}$. The density operator is a normalized Hermitian operator, so $\mathrm{Tr}(\hat{\rho}) = 1$, and it is non-negative (i.e., it has only non-negative eigenvalues) because

$$\langle\phi|\hat{\rho}|\phi\rangle = \sum_k \rho_k |\langle\phi|\psi_k\rangle|^2 \geq 0 \tag{1.20}$$

for any $|\phi\rangle$. Note that the states $|\psi_k\rangle$ in the mixture $\hat{\rho}$ need not be orthogonal to each other. Further, the mixed-state decomposition is not unique. However, when the density operator of Eq. (1.18) is written in its eigenbasis, we find

$$\mathrm{Tr}(\hat{\rho}^2) = \sum_k \rho_k^2 \leq \sum_k \rho_k = 1 \,, \tag{1.21}$$

with ρ_k now being the eigenvalues of $\hat{\rho}$. Equality, $\mathrm{Tr}(\hat{\rho}^2) = 1$, only holds for pure states. Therefore, any state with $\mathrm{Tr}(\hat{\rho}^2) < 1$ is mixed. Alternatively, this becomes manifest in the von Neumann entropy of a state,

$$\begin{aligned} S(\hat{\rho}) &\equiv -\mathrm{Tr}\hat{\rho}\log\hat{\rho} \\ &= -\mathrm{Tr}\left[\sum_k \rho_k|\psi_k\rangle\langle\psi_k|\sum_l(\log\rho_l)|\psi_l\rangle\langle\psi_l|\right] = -\sum_k \rho_k\log\rho_k \ . \end{aligned} \tag{1.22}$$

It becomes nonzero for any mixed state and vanishes for pure states.

1.2.1 Qubit

We shall now consider specific quantum states as they are typically used in quantum information. In a two-dimensional Hilbert space, a general pure qubit state can be written as

$$|\psi_{\theta,\phi}\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)e^{i\phi}|1\rangle \ . \tag{1.23}$$

This state can also be represented in terms of the Bloch vector representation,

$$\begin{aligned} \hat{\rho} &= |\psi_{\theta,\phi}\rangle\langle\psi_{\theta,\phi}| \\ &= \frac{1}{2}\mathbb{1} + \frac{1}{2}\begin{pmatrix} \cos\theta & \sin\theta\, e^{-i\phi} \\ \sin\theta\, e^{+i\phi} & -\cos\theta \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} 1+s_3 & s_1 - is_2 \\ s_1 + is_2 & 1-s_3 \end{pmatrix} = \frac{1}{2}(\mathbb{1} + \boldsymbol{s}\cdot\boldsymbol{\sigma}) \ , \end{aligned} \tag{1.24}$$

with $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \sigma_3)^T$, the Pauli matrices

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{1.25}$$

and

$$\boldsymbol{s} = (s_1, s_2, s_3) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta) \ . \tag{1.26}$$

The Bloch vector $\boldsymbol{s}$ fully describes the qubit state. It points in the direction specified by the spherical coordinates θ and ϕ. The vector's tip lies on the surface of the Bloch sphere, representing a pure state with $|\boldsymbol{s}| = 1$. For mixed states, we would have $|\boldsymbol{s}| < 1$. Throughout, we will interchangeably use $\{\sigma_1, \sigma_2, \sigma_3\}$, $\{\sigma_x, \sigma_y, \sigma_z\}$, and $\{X, Y, Z\}$, respectively, to express the Pauli matrices and operators (where $Y = iXZ$).

A particularly important set of pure qubit states are the six $+1$ eigenstates of $\{\pm X, \pm Y, \pm Z\}$, according to[9]

$$\pm X|\pm\rangle = |\pm\rangle \ , \quad (-1)^k Z|k\rangle = |k\rangle \ , \tag{1.27}$$

[9] For a definition of stabilizers, see the discussion and the box in Section 1.9.

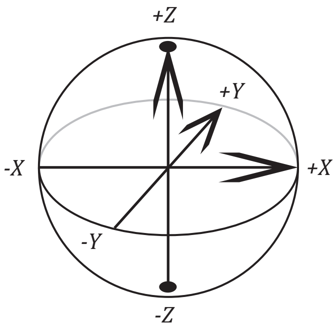

Figure 1.2 The qubit Bloch sphere. There are six $+1$ eigenstates of the Pauli operators $\{\pm X, \pm Y, \pm Z\}$ corresponding to three pairs of basis vectors on opposite sides of the Bloch sphere.

and $\pm Y(|0\rangle \pm \mathrm{i}|1\rangle)/\sqrt{2} = (|0\rangle \pm \mathrm{i}|1\rangle)/\sqrt{2}$, with $k = 0, 1$ and $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$. These are the so-called *stabilizer* states for one qubit, where each pair represents a basis situated on opposite sides of the Bloch sphere (see Figure 1.2). Typically, the Z eigenstates are chosen to be the computational basis, while the X eigenstates are then obtained through Hadamard transformation, $H|k\rangle = (|0\rangle + (-1)^k|1\rangle)/\sqrt{2}$.

1.2.2 Qumode

A natural way to encode quantum information is in terms of quantized harmonic oscillators. In general, we shall refer to these quantum objects as qumodes. In this case, the Hilbert space vectors live in an infinite-dimensional Hilbert space. The observables are Hermitian operators with a discrete, countable or a continuous spectrum such as occupation number or amplitude and phase of the oscillator, respectively. These mathematical notions have their physical interpretation in the complementary particle and wave properties of a quantum oscillator.

The well-known Hamiltonian of a single qumode is $\hbar\omega(\hat{n}+1/2)$, with the Hermitian occupation number operator $\hat{n} \equiv \hat{a}^\dagger\hat{a}$. The eigenstates of the number operator are the number states $|n\rangle$,

$$\hat{n}|n\rangle = n|n\rangle \,, \tag{1.28}$$

where $n = 0, 1, 2, \ldots, \infty$ is the occupation or excitation number of the oscillator. The ground state of the oscillator is defined by

$$\hat{a}|0\rangle = 0 \,. \tag{1.29}$$

The energy $\hbar\omega/2$ corresponds to the ground-state or zero-point energy which is still present when the qumode has an excitation number zero.

The non-Hermitian operators $\hat{a}$ and $\hat{a}^\dagger$ are the lowering and raising operators, respectively,

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle \,, \qquad \hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle \,. \tag{1.30}$$

By successive application of the raising operator, all number states can be obtained from the ground state,

$$|n\rangle = \frac{\left(\hat{a}^\dagger\right)^n}{\sqrt{n!}}|0\rangle \ . \tag{1.31}$$

The number states form an orthonormal,[10]

$$\langle n|m\rangle = \delta_{nm} \ , \tag{1.32}$$

and complete basis,

$$\sum_{n=0}^{\infty} |n\rangle\langle n| = \mathbb{1} \ . \tag{1.33}$$

The Hamiltonian of a single qumode, $\hat{H} = \hbar\omega(\hat{a}^\dagger\hat{a} + 1/2)$, may be rewritten as,

$$\hat{H} = \frac{1}{2}\left(\hat{p}^2 + \omega^2\hat{x}^2\right), \tag{1.34}$$

with

$$\hat{a} = \frac{1}{\sqrt{2\hbar\omega}}(\omega\hat{x} + \mathrm{i}\hat{p}), \quad \hat{a}^\dagger = \frac{1}{\sqrt{2\hbar\omega}}(\omega\hat{x} - \mathrm{i}\hat{p}) \ , \tag{1.35}$$

or, conversely,

$$\hat{x} = \sqrt{\frac{\hbar}{2\omega}}\left(\hat{a} + \hat{a}^\dagger\right), \quad \hat{p} = -\mathrm{i}\sqrt{\frac{\hbar\omega}{2}}\left(\hat{a} - \hat{a}^\dagger\right) \ , \tag{1.36}$$

using the well-known commutation relation for "position" and "momentum",

$$[\hat{x}, \hat{p}] = \mathrm{i}\hbar \ . \tag{1.37}$$

These Hermitian operators are the position and momentum operators of an oscillator with unit mass. The lowering and raising operators satisfy the commutator $[\hat{a}, \hat{a}^\dagger] = 1$. In Eq. (1.35), we see that up to some dimensional factors, the position and momentum operators are the Hermitian real and imaginary parts of the lowering operator. It is then convenient to define the *dimensionless* pair of conjugate quantum variables,

$$\hat{X} \equiv \sqrt{\frac{\omega}{2\hbar}}\hat{x} = \mathrm{Re}\hat{a} \ , \qquad \hat{P} \equiv \frac{1}{\sqrt{2\hbar\omega}}\hat{p} = \mathrm{Im}\hat{a} \ . \tag{1.38}$$

Their commutation relation is given by

$$[\hat{X}, \hat{P}] = \frac{\mathrm{i}}{2} \ . \tag{1.39}$$

[10] The proper normalization is ensured by the prefactors in Eq. (1.30).

In other words, the dimensionless "position" and "momentum" operators, $\hat{X}$ and $\hat{P}$, are defined as if we set $\hbar = 1/2$. Considering a classical oscillator, they would correspond to the real and imaginary parts of the oscillator's complex amplitude. Throughout the text, we use $\hat{x} \equiv \hat{X}$ and $\hat{p} \equiv \hat{P}$ to express the dimensionless position and momentum operators so that $\hat{a} = \hat{x} + \mathrm{i}\hat{p}$.

The Heisenberg uncertainty relation for the variances of two non-commuting observables $\hat{A}$ and $\hat{B}$ in a given quantum state,

$$\begin{aligned} \langle(\Delta\hat{A})^2\rangle &\equiv \langle(\hat{A} - \langle\hat{A}\rangle)^2\rangle = \langle\hat{A}^2\rangle - \langle\hat{A}\rangle^2 \ , \\ \langle(\Delta\hat{B})^2\rangle &\equiv \langle(\hat{B} - \langle\hat{B}\rangle)^2\rangle = \langle\hat{B}^2\rangle - \langle\hat{B}\rangle^2 \ , \end{aligned} \tag{1.40}$$

becomes

$$\langle(\Delta\hat{A})^2\rangle\langle(\Delta\hat{B})^2\rangle \geq \frac{1}{4}|\langle[\hat{A}, \hat{B}]\rangle|^2 \ . \tag{1.41}$$

Inserting Eq. (1.39) into Eq. (1.41) gives the uncertainty relation for a pair of conjugate phase-space variables of a single qumode,

$$\hat{x} = (\hat{a} + \hat{a}^\dagger)/2 \ , \qquad \hat{p} = (\hat{a} - \hat{a}^\dagger)/2\mathrm{i} \ , \tag{1.42}$$

namely,

$$\langle(\Delta\hat{x})^2\rangle\langle(\Delta\hat{p})^2\rangle \geq \frac{1}{4}|\langle[\hat{x}, \hat{p}]\rangle|^2 = \frac{1}{16} \ . \tag{1.43}$$

A single qumode has position and momentum eigenstates,

$$\hat{x}|x\rangle = x|x\rangle \ , \qquad \hat{p}|p\rangle = p|p\rangle \ . \tag{1.44}$$

These are orthogonal,

$$\langle x|x'\rangle = \delta(x - x') \ , \qquad \langle p|p'\rangle = \delta(p - p') \ , \tag{1.45}$$

and complete,

$$\int\limits_{-\infty}^{\infty} |x\rangle\langle x|\mathrm{d}x = \mathbb{1} \ , \qquad \int\limits_{-\infty}^{\infty} |p\rangle\langle p|\mathrm{d}p = \mathbb{1} \ , \tag{1.46}$$

and they would correspond to lines in phase space, as shown in Figure 1.3.

As it is well-known from quantum mechanics, the position and momentum eigenstates are related to each other by the Fourier transformation,

$$|x\rangle = \frac{1}{\sqrt{\pi}} \int\limits_{-\infty}^{\infty} \mathrm{e}^{-2\mathrm{i}xp}|p\rangle\mathrm{d}p \ , \qquad |p\rangle = \frac{1}{\sqrt{\pi}} \int\limits_{-\infty}^{\infty} \mathrm{e}^{+2\mathrm{i}xp}|x\rangle\mathrm{d}x \ . \tag{1.47}$$

The Fourier transformation of a qumode is the analogue of the discrete Hadamard gate for a qubit mentioned in the preceding section (see Figure 1.4). Similarly, $|x\rangle$

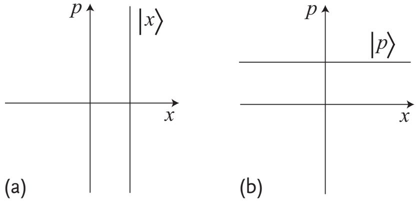

Figure 1.3 *Z* and *X* stabilizer states of a qumode in phase space. (a) Computational position basis, (b) conjugate momentum basis.

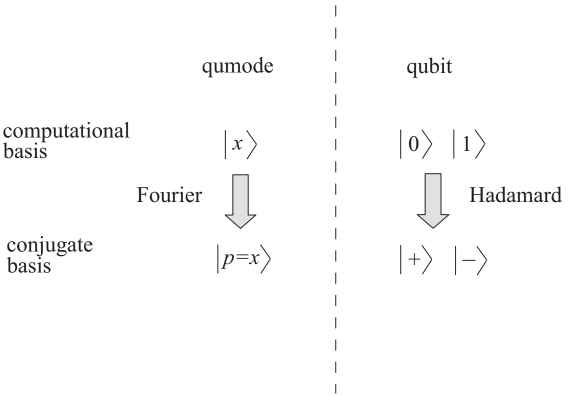

Figure 1.4 Basis state transformations for a qumode and a qubit. $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$.

and $|p\rangle$ play the roles of the computational and the conjugate basis, respectively, like $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ in the qubit case. They are the eigenstates of the Weyl–Heisenberg (WH) operators,

$$X(s) \equiv \mathrm{e}^{-2\mathrm{i}s\hat{p}}\,, \qquad Z(s) \equiv \mathrm{e}^{+2\mathrm{i}s\hat{x}}\,, \tag{1.48}$$

with

$$\mathrm{e}^{+2\mathrm{i}sp} X(s)|p\rangle = |p\rangle\,, \qquad \mathrm{e}^{-2\mathrm{i}sx} Z(s)|x\rangle = |x\rangle\,, \tag{1.49}$$

similar to Eq. (1.27) for a single qubit. The position and momentum states, being the above $+1$ WH eigenstates, are among the stabilizer states[11] for a single qumode. A more general set of stabilizer states would include rotated position or momentum eigenstates. For instance, the rotated p-momentum states are $+1$ eigenstates of

$$\mathrm{e}^{+2\mathrm{i}sp-\mathrm{i}s^2\cos\theta\sin\theta} X(s\cos\theta) Z(-s\sin\theta) \equiv g_p^{(\theta)}(s)\,, \tag{1.50}$$

with a "clockwise" rotation angle θ. In particular, by using our convention, for $\theta = -\pi/2$, we recover the stabilizer of the position states (here with eigenvalue

[11] For a definition of stabilizers, see the discussion and the box in Section 1.9.

$-p$) corresponding to a Fourier transformation of the p-momentum states. We shall get back to these qumode stabilizers later in various contexts such as unitaries on qumodes and optical Gaussian states of one or more qumodes.

A general pure qumode state $|\psi\rangle$ can be expanded in the position basis,

$$|\psi\rangle = \int \mathrm{d}x |x\rangle\langle x|\psi\rangle = \int \mathrm{d}x\, \psi(x)|x\rangle \ , \tag{1.51}$$

where $\langle x|\psi\rangle = \psi(x)$ is the position wave function. Any mixed state may be written as

$$\hat{\rho} = \int f(s,t) X(s) Z(t) \mathrm{d}s\, \mathrm{d}t \ , \tag{1.52}$$

with a complex function $f(s,t)$. In quantum optics, this would correspond to a phase-space expansion in terms of the quantum optical displacement operator.

Encoding quantum information

⊙ **Qubit:**

arbitrary pure states:

$$|\psi_{\theta,\phi}\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)\mathrm{e}^{\mathrm{i}\phi}|1\rangle$$

arbitrary mixed states:

$$\hat{\rho} = \frac{1}{2}(\mathbb{1} + \boldsymbol{s}\cdot\boldsymbol{\sigma}) \ , \quad \boldsymbol{\sigma} = (\sigma_1, \sigma_2, \sigma_3)^{\mathrm{T}} \ , \quad |\boldsymbol{s}| \le 1$$

stabilizer states as $+1$ eigenstates of $\{\pm X \equiv \pm\sigma_1, \pm Y \equiv \pm\sigma_2, \pm Z \equiv \pm\sigma_3\}$:

$$\pm X(|0\rangle \pm |1\rangle)/\sqrt{2} = (|0\rangle \pm |1\rangle)/\sqrt{2}$$
$$\pm Y(|0\rangle \pm \mathrm{i}|1\rangle)/\sqrt{2} = (|0\rangle \pm \mathrm{i}|1\rangle)/\sqrt{2}$$
$$+Z|0\rangle = |0\rangle \ , \quad -Z|1\rangle = |1\rangle$$

with qubit Pauli operators X, Y, Z

∿∿∿ **Qumode:**

arbitrary pure states:

$$|\psi\rangle = \int \mathrm{d}x\, \psi(x)|x\rangle$$

arbitrary mixed states:

$$\hat{\rho} = \int \mathrm{d}s\, \mathrm{d}t\, f(s,t) X(s) Z(t)$$

stabilizer states as $+1$ eigenstates of $\{\mathrm{e}^{+2\mathrm{i}sp} X(s), \mathrm{e}^{-2\mathrm{i}sx} Z(s)\}$:

$$\mathrm{e}^{+2\mathrm{i}sp} X(s)|p\rangle = |p\rangle$$
$$\mathrm{e}^{-2\mathrm{i}sx} Z(s)|x\rangle = |x\rangle$$

with qumode Weyl–Heisenberg operators $X(s) = \mathrm{e}^{-2\mathrm{i}s\hat{p}}$ and $Z(s) = \mathrm{e}^{+2\mathrm{i}s\hat{x}}$

A general physical operation on a density operator can be non-unitary, including irreversible channels and measurements. However, reversibly mapping a normalized density operator onto another normalized density operator is described by unitaries which we briefly discuss in the following section.

1.3 Unitaries

Unitary transformations (unitaries) represented by unitary operators $\hat{U}$, with $\hat{U}^\dagger \hat{U} = \hat{U}\hat{U}^\dagger = \mathbb{1}$, preserve the norms and overlaps of states. However, this trace-preserving property is not the most distinct feature of unitaries. Rather, it is reversibility.[12] By acting on Hilbert space vectors, unitaries are used in order to access any other vector in the same Hilbert space; an important tool for quantum computation.[13]

As it is well-known from standard quantum mechanics, the unitary evolution of a quantum system can be described in the Schrödinger as well as the Heisenberg representation. Assume the pure state $|\psi(t_0)\rangle$ is prepared at time t_0. The unitarily evolved state at time $t > t_0$ can then be written in the Schrödinger representation as

$$|\psi(t)\rangle = \hat{U}(t, t_0)|\psi(t_0)\rangle \, . \tag{1.53}$$

For a closed system where the Hamiltonian is time independent, $\partial \hat{H}/\partial t = 0$, the unitary operator $\hat{U}(t, t_0)$ takes on the simple form

$$\hat{U}(t, t_0) = \exp\left[-\frac{\mathrm{i}}{\hbar}\hat{H}(t - t_0)\right] \, . \tag{1.54}$$

The unitary evolution of a mixed state is easily found to be

$$\hat{\rho}(t) = \hat{U}(t, t_0)\hat{\rho}(t_0)\hat{U}^\dagger(t, t_0) \, , \tag{1.55}$$

using Eq. (1.18).

In the Heisenberg representation, the initial states remain unchanged during the evolution, $|\psi_{\mathrm{H}}(t)\rangle \equiv |\psi_{\mathrm{H}}\rangle = |\psi(t_0)\rangle$. It follows $|\psi_{\mathrm{H}}\rangle = \hat{U}^\dagger(t, t_0)|\psi(t)\rangle$. Equivalence of the expectation values in both representations means

$$\begin{aligned}\langle\psi_{\mathrm{H}}|\hat{M}_{\mathrm{H}}(t)|\psi_{\mathrm{H}}\rangle &= \langle\psi(t)|\hat{U}(t, t_0)\hat{U}^\dagger(t, t_0)\hat{M}\hat{U}(t, t_0)\hat{U}^\dagger(t, t_0)|\psi(t)\rangle \\ &= \langle\psi(t)|\hat{M}|\psi(t)\rangle \, ,\end{aligned} \tag{1.56}$$

for arbitrary $|\psi_{\mathrm{H}}\rangle$. Thus, we obtain

$$\hat{M}_{\mathrm{H}}(t) = \hat{U}^\dagger(t, t_0)\hat{M}\hat{U}(t, t_0) \, . \tag{1.57}$$

[12] Which refers to physical reversibility; a notion stronger than just mathematical invertibility.

[13] Later, however, we shall describe the one-way model of quantum computation which achieves this universal accessibility of quantum states in an irreversible fashion through measurements on an entangled resource state.

This corresponds to the equation of motion

$$\frac{\mathrm{d}}{\mathrm{d}t}\hat{M}_{\mathrm{H}}(t) = \frac{1}{\mathrm{i}\hbar}\hat{U}^{\dagger}[\hat{M}, \hat{H}]\hat{U} + \hat{U}^{\dagger}\frac{\partial \hat{M}}{\partial t}\hat{U} , \tag{1.58}$$

or

$$\mathrm{i}\hbar\frac{\mathrm{d}}{\mathrm{d}t}\hat{M}_{\mathrm{H}}(t) = \left[\hat{M}_{\mathrm{H}}, \hat{H}_{\mathrm{H}}\right] + \mathrm{i}\hbar\frac{\partial \hat{M}_{\mathrm{H}}}{\partial t} . \tag{1.59}$$

Therefore, the action of an arbitrary unitary operator $\hat{U}$ is described by either $\hat{M} \to \hat{U}^{\dagger}\hat{M}\hat{U}$ (Heisenberg) or $\hat{\rho} \to \hat{U}\hat{\rho}\hat{U}^{\dagger}$ (Schrödinger). Here, we dropped the time dependence, focusing on an input–output relation between states or observables.

1.3.1 Qubit

Consider a single qubit. According to the Bloch sphere representation in Figure 1.2, it is convenient to think of single-qubit unitaries as rotations. In particular, finite rotations around the coordinate axes are expressed by

$$\hat{R}_{s}(\theta) = \mathrm{e}^{-\mathrm{i}\theta\, s\cdot\boldsymbol{\sigma}/2} = \cos(\theta/2)\mathbb{1} - \mathrm{i}\sin(\theta/2)\boldsymbol{s}\cdot\boldsymbol{\sigma} , \tag{1.60}$$

again with $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \sigma_3)^{\mathrm{T}}$ for the Pauli operators $\{\sigma_1, \sigma_2, \sigma_3\} \equiv \{X, Y, Z\}$ and the real unit vector $\boldsymbol{s}$ (thus, strictly $|\boldsymbol{s}| = 1$), using $(\boldsymbol{s}\cdot\boldsymbol{\sigma})^2 = \mathbb{1}$. For example, a rotation around the Z-axis corresponds to $\hat{R}_{(0,0,1)}(\theta) \equiv \hat{R}_{Z}(\theta) = \mathrm{e}^{-\mathrm{i}\theta Z/2} \equiv Z_{\theta}$. In the Heisenberg representation, it becomes clear that the rotation takes place in the XY-plane,

$$\begin{aligned} Z_{\theta}^{\dagger}XZ_{\theta} &= Z_{-\theta}XZ_{\theta} = X\cos\theta - Y\sin\theta , \\ Z_{\theta}^{\dagger}YZ_{\theta} &= Z_{-\theta}YZ_{\theta} = X\sin\theta + Y\cos\theta , \\ Z_{\theta}^{\dagger}ZZ_{\theta} &= Z_{-\theta}ZZ_{\theta} = Z . \end{aligned} \tag{1.61}$$

Another thing becomes apparent here. Two different, though discrete choices of the rotation angle, for instance, $\theta = \pi/2$ and $\theta = \pi/4$, lead to very distinct output operators: while $\theta = \pi/2$ transforms the Pauli operators into Pauli operators, the choice of $\theta = \pi/4$ results in linear combinations of Pauli operators.

The set of single-qubit unitaries that transform Pauli operators into Pauli operators,

$$\left\{\hat{U} | \hat{U}^{\dagger}\sigma_k\hat{U} = \pm\sigma_l\right\} , \tag{1.62}$$

forms a group, the so-called *Clifford* group. Clifford group elements map stabilizer states $|S\rangle$ onto stabilizer states $|S'\rangle$.[14] Assume $g, g' \in \{\pm X, \pm Y, \pm Z\}$ such that

[14] The corresponding stabilizer group S is an abelian subgroup of the one-qubit Pauli group, $\{\pm\mathbb{1}, \pm i\mathbb{1}, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$. The prefactors $(\pm i)$ which ensure that the Pauli group is closed under multiplication are not important for our purposes and will be omitted throughout. For a detailed definition of stabilizers see Section 1.9.

$g|S\rangle = |S\rangle$ and $g'|S'\rangle = |S'\rangle$. Then, we obtain the Clifford transformed state

$$\hat{U}|S\rangle = \hat{U}g|S\rangle = \hat{U}g\hat{U}^\dagger\hat{U}|S\rangle = \hat{U}g\hat{U}^\dagger|S'\rangle = g'|S'\rangle \,. \tag{1.63}$$

Thus, the inverse Heisenberg evolution of the corresponding single-qubit stabilizer, $g \in \{\pm X, \pm Y, \pm Z\} \rightarrow g' = \hat{U}g\hat{U}^\dagger \in \{\pm X, \pm Y, \pm Z\}$, completely determines the resulting state $|S'\rangle$. For example,

$$Z_{\pi/2}|+\rangle = \left(\mathrm{e}^{-\mathrm{i}\pi/4}|0\rangle + \mathrm{e}^{+\mathrm{i}\pi/4}|1\rangle\right)/\sqrt{2} = \mathrm{e}^{-\mathrm{i}\pi/4}(|0\rangle + \mathrm{i}|1\rangle)/\sqrt{2}\,, \tag{1.64}$$

corresponds to

$$X \rightarrow Z_{\pi/2}XZ_{-\pi/2} = Y\,, \tag{1.65}$$

up to an irrelevant phase factor. The distinction between Clifford unitaries and non-Clifford unitaries will be important regarding universality and nonclassical speed-up in quantum computation (see Section 1.8).

1.3.2 Qumode

Now, consider a single qumode. In this case, the free evolution of the oscillator is a rotation in phase space. Using the input–output formalism, such a phase rotation of a single qumode with annihilation operator $\hat{a}$ can be expressed by

$$\hat{a} \rightarrow \hat{R}^\dagger(\theta)\hat{a}\hat{R}(\theta) = \hat{a}\mathrm{e}^{-\mathrm{i}\theta}\,, \tag{1.66}$$

with

$$\hat{R}(\theta) = \exp\left(-\mathrm{i}\theta\,\hat{a}^\dagger\hat{a}\right). \tag{1.67}$$

In terms of the position and momentum operators (recall that $\hat{a} = \hat{x} + \mathrm{i}\hat{p}$), we obtain

$$\begin{aligned}\hat{R}^\dagger(\theta)\hat{x}\hat{R}(\theta) &= \hat{x}\cos\theta + \hat{p}\sin\theta\,,\\ \hat{R}^\dagger(\theta)\hat{p}\hat{R}(\theta) &= -\hat{x}\sin\theta + \hat{p}\cos\theta\,.\end{aligned} \tag{1.68}$$

In this case, the resulting operators are always linear combinations of the input operators for any choice of θ. The phase-rotation unitary is an element of the Clifford group which, for qumodes, may be defined similar to the qubit case as

$$\left\{\hat{U}|\,\hat{U}^\dagger X_k(s)\hat{U} \propto X_l(s)\right\}. \tag{1.69}$$

In this case, $X_k(s)$ and $X_l(s)$ stand for products of WH operators, that is, products of elements of the WH group. Thus, the Clifford single-qumode unitaries transform WH operators into products of WH operators. In terms of the WH group generators, that is, the momentum and position operators, Clifford transformations always lead to linear combinations of the generators. Non-Clifford transformations result in nonlinear combinations of $\hat{x}$ and $\hat{p}$.

We observe that general single-qubit rotations on the Bloch sphere do contain non-Clifford elements, whereas single-qumode rotations in phase space do not.[15] In the qubit case, the rotation angle determines whether a unitary is Clifford or not. For qumodes, the Clifford or non-Clifford character of a unitary $\hat{U}$ depends on the order of the Hamiltonian that generates $\hat{U}$. We shall return to this discussion later.

The above discussion on transforming stabilizer states through Clifford unitaries applies as well to qumodes. Stabilizer states $|S\rangle$ are then mapped onto stabilizer states $|S'\rangle$. The stabilizers this time, represented by $g(s)$ and $g'(s)$, are products of WH operators. Again, the inverse Heisenberg evolution of the corresponding single-qumode stabilizer, $g(s) \to g'(s) = \hat{U} g(s) \hat{U}^\dagger$, completely determines the resulting state $|S'\rangle$. For example, the Fourier transform of a p-momentum eigenstate, with $\hat{F} \equiv \hat{R}(-\pi/2)$ in our convention, leads to an x-position eigenstate with eigenvalue $-p$, $\hat{F}|p\rangle = |x = -p\rangle$. This corresponds to

$$e^{+2isp} X(s) \to e^{+2isp} \hat{F} X(s) \hat{F}^\dagger = e^{+2isp} Z(s) \,, \tag{1.70}$$

using $\hat{F}\hat{p}\hat{F}^\dagger = -\hat{x}$. More generally, an arbitrary rotation $\hat{R}(\theta)$ acting, for instance, on a p-momentum eigenstate, gives the state $\hat{R}(\theta)|p\rangle$ which is stabilized by

$$\begin{aligned} \hat{R}(\theta) e^{+2isp} X(s) \hat{R}^\dagger(\theta) &= e^{+2isp} e^{-2is\left(\hat{p}\cos\theta + \hat{x}\sin\theta\right)} \\ &= e^{+2isp} e^{-2is\hat{p}\cos\theta} e^{-2is\hat{x}\sin\theta} e^{-2[is\hat{p}\cos\theta, is\hat{x}\sin\theta]} \\ &= g_p^{(\theta)}(s) \,, \end{aligned} \tag{1.71}$$

as defined earlier in Eq. (1.50). Here, we used the well-known Baker–Campbell–Hausdorff formula, $e^{\hat{A}+\hat{B}} = e^{\hat{A}} e^{\hat{B}} e^{-[\hat{A},\hat{B}]/2}$ for $[\hat{A}, [\hat{A}, \hat{B}]] = 0$, and so on, and the input–output relations in Eq. (1.68). General single-qumode Clifford unitaries also include squeezers beside the phase rotations. Squeezing applied to an unphysical, qumode stabilizer state corresponds to a rescaling of the eigenvalue. For instance, for a squeezing operation $\hat{S}(-r)$ acting on a p-momentum eigenstate, we obtain the new stabilizer

$$\hat{S}(-r) e^{+2isp} X(s) \hat{S}^\dagger(-r) = e^{+2isp} X(s e^{+r}) \,, \tag{1.72}$$

using $\hat{S}(-r)\hat{p}\hat{S}^\dagger(-r) = e^{+r}\hat{p}$ [see Eq. (2.52) through Eq. (2.56)]. Therefore, the new stabilizer state is $|e^{-r} p\rangle$ since we have $e^{+2isp} X(s e^{+r}) |e^{-r} p\rangle = |e^{-r} p\rangle$.

[15] This is a first hint that single-qubit non-Clifford unitaries might be optically easy to implement, while those for a single qumode are hard to realize. This is, however, compensated by the complication of making two photons interact for a two-qubit entangling gate, whereas entangling two qumodes is relatively easy. The next chapter will provide additional details on this issue.

Reversible quantum operations

state $\hat{\rho} \to \hat{U}\hat{\rho}\hat{U}^\dagger$ (Schrödinger), observable $\hat{M} \to \hat{U}^\dagger\hat{M}\hat{U}$ (Heisenberg)

$$\langle \hat{M} \rangle = \mathrm{Tr}(\hat{\rho}\hat{M}) \to \mathrm{Tr}[(\hat{U}\hat{\rho}\hat{U}^\dagger)\hat{M}] = \mathrm{Tr}[\hat{\rho}(\hat{U}^\dagger\hat{M}\hat{U})] \quad \text{and}$$
$$\hat{U}\hat{U}^\dagger = \hat{U}^\dagger\hat{U} = \mathbb{1}$$

⊙ **Qubit:** arbitrary unitaries:

$$e^{i\phi}\hat{R}_s(\theta) = e^{i\phi}e^{-i\theta\, \boldsymbol{s}\cdot\boldsymbol{\sigma}/2} = e^{i\phi}\left[\cos(\theta/2)\mathbb{1} - i\sin(\theta/2)\boldsymbol{s}\cdot\boldsymbol{\sigma}\right], \quad |\boldsymbol{s}| = 1$$

with $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \sigma_3)^{\mathrm{T}}$ and the Pauli operators $\{X \equiv \sigma_1, Y \equiv \sigma_2, Z \equiv \sigma_3\}$

Clifford unitaries:

$$g \in \{\pm X, \pm Y, \pm Z\} \to g' = \hat{U}g\hat{U}^\dagger \in \{\pm X, \pm Y, \pm Z\}$$

with $g|S\rangle = |S\rangle$ and $g'|S'\rangle = |S'\rangle$ for qubit stabilizer states $|S\rangle, |S'\rangle = \hat{U}|S\rangle$

〰 **Qumode:** arbitrary unitaries:

$$\hat{U} = e^{-it\,H(\hat{a},\hat{a}^\dagger)},\ H(\hat{a},\hat{a}^\dagger) \quad \text{is arbitrary Hamiltonian ,}$$
$$\hat{a} \to \hat{U}^\dagger\hat{a}\hat{U} \quad \text{is nonlinear transformation}$$

Clifford unitaries:

$$\left\{\hat{U} |\, \hat{U}^\dagger X_k(s)\hat{U} \propto X_l(s)\right\}$$

with $X_k(s)$ and $X_l(s)$ products of WH operators and

$$\hat{U} = e^{-it\,H(\hat{a},\hat{a}^\dagger)},\ H(\hat{a},\hat{a}^\dagger) \quad \text{is quadratic Hamiltonian ,}$$
$$\hat{a} \to \hat{U}^\dagger\hat{a}\hat{U} \quad \text{is linear transformation}$$

The qumode Clifford unitaries, combining squeezing, rotations, and displacements, are useful for defining a universal gate set (see later in Section 1.8).

Squeezing itself will become an important tool when we discuss physical qumode stabilizer states, that is, Gaussian states, in the next chapter. While any qumode Clifford unitary can be generated by a Hamiltonian which is a quadratic polynomial of $\hat{x}$, $\hat{p}$ or $\hat{a}$, $\hat{a}^\dagger$, a general qumode unitary requires a Hamiltonian of sufficiently high order. An at least cubic Hamiltonian suffices to realize arbitrary qumode unitaries asymptotically (see Section 1.8).

In the next section, we will discuss quantum operations which do not belong to the class of unitaries. These are the irreversible channels and measurements.

1.4 Non-unitaries

A physical, generally non-unitary quantum operation corresponds to a linear map between density operators, $\hat{\rho} \to \hat{\rho}' = \mathcal{E}(\hat{\rho})$.

For this linear map to be physical, it must satisfy the mathematical notion of *complete positivity*. Such a completely positive (CP) map can always be written in the form of an operator sum,

$$\mathcal{E}(\hat{\rho}) = \sum_k \hat{A}_k \hat{\rho} \hat{A}_k^\dagger \,. \tag{1.73}$$

The sum may be finite or go to infinity and the summation over k may also be replaced by an integral. The operators $\hat{A}_k$ are usually referred to as Kraus operators. When the corresponding set of positive operators $\hat{A}_k^\dagger \hat{A}_k$ sums up to the identity, $\sum_k \hat{A}_k^\dagger \hat{A}_k = \mathbb{1}$, we have a CP trace-preserving (CPTP) map. Otherwise, when $\sum_k \hat{A}_k^\dagger \hat{A}_k < \mathbb{1}$, the CP map is trace-decreasing (CPTD).

This distinction leads to an output density operator which is either normalized or not. In the former case, the corresponding CPTP map describes an, in general, irreversible channel. The case of an unnormalized output after a CPTD map represents situations where information is gained through measurements and hence a certain output state is only obtained with non-unit probability. The following two sections are devoted to this distinction of channels and measurements. In the next section, we will also explain the important difference between positivity and complete positivity.

1.4.1 Channels

Consider a signal system A in a state $\hat{\rho}_{\mathrm{A}}$. Now, suppose the signal interacts with an ancilla system B in a state $\hat{\rho}_{\mathrm{B}}$ through a global unitary $\hat{U}_{\mathrm{AB}}$ (see Figure 1.5). When the ancilla is traced over, the effect of this transformation on the signal is described by

$$\begin{aligned}
\hat{\rho}_{\mathrm{A}} \to \hat{\rho}_{\mathrm{A}}' &= \mathrm{Tr}_{\mathrm{B}}\left[\hat{U}_{\mathrm{AB}}\left(\hat{\rho}_{\mathrm{A}} \otimes \hat{\rho}_{\mathrm{B}}\right)\hat{U}_{\mathrm{AB}}^\dagger\right] \\
&= \sum_k {}_{\mathrm{B}}\langle k|\hat{U}_{\mathrm{AB}}\left[\hat{\rho}_{\mathrm{A}} \otimes \left(\sum_l \rho_l |l\rangle_{\mathrm{B}}\langle l|\right)\right]\hat{U}_{\mathrm{AB}}^\dagger |k\rangle_{\mathrm{B}} \\
&= \sum_{k,l}\left({}_{\mathrm{B}}\langle k|\sqrt{\rho_l}\,\hat{U}_{\mathrm{AB}}|l\rangle_{\mathrm{B}}\right)\hat{\rho}_{\mathrm{A}}\left({}_{\mathrm{B}}\langle l|\sqrt{\rho_l}\,\hat{U}_{\mathrm{AB}}^\dagger|k\rangle_{\mathrm{B}}\right) \\
&\equiv \sum_{k,l} \hat{A}_{kl}\hat{\rho}_{\mathrm{A}}\hat{A}_{kl}^\dagger = \mathcal{E}(\hat{\rho}_{\mathrm{A}}) \,,
\end{aligned} \tag{1.74}$$

where we used a diagonal basis $\{|l\rangle_{\mathrm{B}}\}$ to express $\hat{\rho}_{\mathrm{B}}$ and to trace over B. Note that $\hat{A}_{kl}$ is an operator in the Hilbert space of the signal A. For the simple case of an

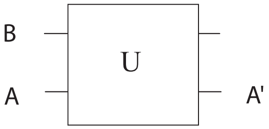

Figure 1.5 A signal system A in an initial state labeled by A interacts with an ancilla system B in an initial state labeled by B through a global unitary U. The resulting signal state is labeled by A′ after tracing over system B.

ancilla starting in the state $\hat{\rho}_{\mathrm{B}} = |0\rangle_{\mathrm{B}}\langle 0|$, that is, $\rho_k = \delta_{k0}$, we obtain the operator sum in Eq. (1.73) with $\hat{A}_k \equiv {}_{\mathrm{B}}\langle k|\hat{U}_{\mathrm{AB}}|0\rangle_{\mathrm{B}}$ and the signal density operators $\hat{\rho} \equiv \hat{\rho}_{\mathrm{A}}$.[16)]

The *operator sum* or Kraus representation in Eq. (1.73) represents a CPTP map. The TP property is easily confirmed through

$$\begin{aligned}\mathrm{Tr}\mathcal{E}(\hat{\rho}) &= \mathrm{Tr}\left(\sum_k \hat{A}_k\hat{\rho}\hat{A}_k^\dagger\right) = \sum_k \mathrm{Tr}\left(\hat{A}_k^\dagger\hat{A}_k\hat{\rho}\right)\\ &= \mathrm{Tr}\left[\left(\sum_k \hat{A}_k^\dagger\hat{A}_k\right)\hat{\rho}\right] = 1\ ,\end{aligned} \tag{1.75}$$

provided that $\sum_k \hat{A}_k^\dagger\hat{A}_k = \mathbb{1}$ holds. In the first line of Eq. (1.75), we used the invariance property of the trace operation under cyclic permutations. In order to see that $\sum_k \hat{A}_k^\dagger\hat{A}_k = \mathbb{1}$ is not only sufficient, but also necessary for the TP property of $\mathcal{E}$, note that the last line in Eq. (1.75) must be satisfied for *any* normalized state $\hat{\rho}$.

Let us now explain the CP property of the map $\mathcal{E}$. Clearly, for the output density operator to represent a physical state we need $\mathcal{E}(\hat{\rho}) \geq 0$. However, there are operations that do satisfy this positivity constraint, but nonetheless are unphysical.[17)] Hence, a stricter condition is required, assuming that the signal A is part of a larger composite system A and B. In this case, the condition is $\$_{\mathcal{E}}\,\hat{\rho}_{\mathrm{A}} = \hat{\rho}'_{\mathrm{A}} \geq 0$ *and* $(\$_{\mathcal{E}} \otimes \mathbb{1}_{\mathrm{B}})\hat{\rho}_{\mathrm{AB}} = \hat{\rho}'_{\mathrm{AB}} \geq 0$, where $\$_{\mathcal{E}}$ stands for the (super)operator that affects the map $\mathcal{E}$ on system A.

In conclusion, a map $\mathcal{E}$ that describes a physical operation is CP and linear. Linearity means that $\mathcal{E}[\lambda\hat{\rho}_1 + (1-\lambda)\hat{\rho}_2] = \lambda\mathcal{E}(\hat{\rho}_1) + (1-\lambda)\mathcal{E}(\hat{\rho}_2)$. Whenever the ancilla system B in Figure 1.5 is assumed to be inaccessible such that no information can be gained from it (for instance, when it represents the uncontrollable environment of the signal A), the trace over B gives a new normalized density operator for A; thus, $\mathcal{E}$ is TP. The situation of an accessible ancilla system B that can be measured and acts as a probe to the signal will be considered in the next section.

We introduced CPTP maps in the Schrödinger representation. Similar to the unitary case, we may also describe the reduced dynamics of the signal system in

[16)] Note that the operators $\hat{A}_k$ are not unique and can always be transformed into new operators $\hat{A}'_l = \sum_k u_{lk}\hat{A}_k$ with a unitary matrix u such that $\sum_l \hat{A}'_l\hat{\rho}\hat{A}'^\dagger_l = \sum_{lkm} u_{lk}u^*_{lm}\hat{A}_k\hat{\rho}\hat{A}^\dagger_m = \sum_k \hat{A}_k\hat{\rho}\hat{A}^\dagger_k$ since $\sum_l u^*_{lm}u_{lk} = \delta_{mk}$.

[17)] An example for such an unphysical operation is transposition. It is a positive, but not completely positive TP map. This property turns out to be useful for inseparability checks of bipartite density matrices (see Section 1.5).

the Heisenberg representation,

$$\mathcal{E}^*(\hat{M}) = \sum_k \hat{A}_k^\dagger \hat{M} \hat{A}_k \, , \tag{1.76}$$

where now the *dual map* $\mathcal{E}^*$ is a completely positive unity-preserving (CPUP) map, $\mathcal{E}^*(\mathbb{1}) = \mathbb{1}$, when $\sum_k \hat{A}_k^\dagger \hat{A}_k = \mathbb{1}$, and $\hat{M}$ is an observable. This map is uniquely defined by requiring that the expectation values are independent of the representation, $\langle \hat{M} \rangle = \mathrm{Tr}(\hat{\rho}\hat{M}) \to \mathrm{Tr}[\mathcal{E}(\hat{\rho})\hat{M}] = \mathrm{Tr}[\hat{\rho}\mathcal{E}^*(\hat{M})]$.

In general, the dual map will change the commutators, that is, the algebra is not preserved; a sign for non-unitary evolution. Only for reversible channels, that is, unitaries, the algebra is invariant. For instance, for a single qumode, we have $[\hat{x}, \hat{p}] \to \hat{U}^\dagger[\hat{x}, \hat{p}]\hat{U} = [\hat{U}^\dagger \hat{x} \hat{U}, U^\dagger \hat{p} \hat{U}]$, whereas, in general, $[\hat{x}, \hat{p}] \to \mathcal{E}^*([\hat{x}, \hat{p}]) \neq [\mathcal{E}^*(\hat{x}), \mathcal{E}^*(\hat{p})]$. Similarly, only for unitaries do we have $f(\hat{x}, \hat{p}) \to f(\hat{U}^\dagger \hat{x} \hat{U}, \hat{U}^\dagger \hat{p} \hat{U})$ for arbitrary polynomials $f(\hat{x}, \hat{p})$ (in fact, we used this earlier on). However, under a non-unitary map $\mathcal{E}^*$, in general, $f(\hat{x}, \hat{p})$ evolves into $\mathcal{E}^*(f(\hat{x}, \hat{p})) \neq f(\mathcal{E}^*(\hat{x}), \mathcal{E}^*(\hat{p}))$.[18]

For a general qubit channel expressed by an operator sum, Eq. (1.73), the Kraus operators can be expanded in terms of the Pauli basis. Thus, we have [5]

$$\hat{A}_k = \alpha_k \mathbb{1} + \beta_k X + \gamma_k Y + \delta_k Z \, . \tag{1.77}$$

Similarly, for a general qumode channel, we can use the WH operators as a complete basis such that [28]

$$\mathcal{E}(\hat{\rho}) = \int \mathrm{d}s\mathrm{d}t\mathrm{d}s'\mathrm{d}t' \, f(s, t, s', t') X(s) Z(t) \hat{\rho} X(-s') Z(-t') \, . \tag{1.78}$$

Finally, we note that also for non-unitary dynamics, similar to the case of reversible, unitary dynamics, we may keep track of the continuous time evolution of the states or observables. Such continuous, non-unitary, mixed-state evolutions are given by the well-known master and Langevin equations, respectively [29].[19]

[18] We should at least mention that those dual maps that map the generators $\hat{x}$ and $\hat{p}$ to linear combinations of $\hat{x}$ and $\hat{p}$ (and WH operators to products of WH operators) correspond to the important Gaussian channels in the Schrödinger representation. These will be discussed later in Chapter 2. This particular case of non-unitary reduced dynamics is a kind of mixed-state extension of the Clifford unitaries that transform stabilizer states into stabilizer states, as presented in the preceding section. A mathematically more rigorous discussion of channels, Schrödinger CPTP maps, and Heisenberg CPUP dual maps and other examples can be found in Chapter II.5 of [6].

[19] However, the operator sum representation is in some sense more general, as it even allows one to describe non-Markovian dynamics [5]. The continuous time evolution of the master equation corresponds to the quantum version of a continuous Markov chain while the operator sum is the quantum analogue of a probability map. In particular, for the master equation, the signal A and the ancilla/environment B must not be entangled initially (so-called Markovian approximation). The solution of the master equation can always be written as well as $\hat{\rho}(t) = \sum_k \hat{A}_k(t)\hat{\rho}(0)\hat{A}_k^\dagger(t)$.

Irreversible quantum operations, channels

state $\hat{\rho} \to \mathcal{E}(\hat{\rho}) = \sum_k \hat{A}_k \hat{\rho} \hat{A}_k^\dagger$ (Schrödinger CPTP),
observable $\hat{M} \to \mathcal{E}^*(\hat{M}) = \sum_k \hat{A}_k^\dagger \hat{M} \hat{A}_k$ (Heisenberg CPUP)

$$\langle \hat{M} \rangle = \mathrm{Tr}(\hat{\rho}\hat{M}) \to \mathrm{Tr}\left[\left(\sum_k \hat{A}_k \hat{\rho} \hat{A}_k^\dagger\right)\hat{M}\right] = \mathrm{Tr}\left[\hat{\rho}\left(\sum_k \hat{A}_k^\dagger \hat{M} \hat{A}_k\right)\right]$$

and $\sum_k \hat{A}_k^\dagger \hat{A}_k = \mathbb{1}$

⊙ **Qubit:** arbitrary channels:

$$\hat{A}_k = \alpha_k \mathbb{1} + \beta_k X + \gamma_k Y + \delta_k Z$$

Pauli channels:

$$\hat{A}_k \propto \mathbb{1}, X, Y, Z\ , \quad \forall k\ ,$$

amplitude damping channel:

$$\hat{A}_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \quad \hat{A}_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$$

〰 **Qumode:** arbitrary channels:

$$\mathcal{E}(\hat{\rho}) = \int \mathrm{d}s\mathrm{d}t\mathrm{d}s'\mathrm{d}t'\, f(s,t,s',t')X(s)Z(t)\hat{\rho}X(-s')Z(-t')$$

WH channels:

$$\mathcal{E}(\hat{\rho}) = \int \mathrm{d}s\mathrm{d}t\, f(s,t)X(s)Z(t)\hat{\rho}X(-s)Z(-t)$$

amplitude damping channel:

$$\mathcal{E}(\hat{\rho}) = \sum_{k=0}^{\infty} \hat{A}_k \hat{\rho} \hat{A}_k^\dagger\ , \quad \hat{A}_k = \sum_{n=k}^{\infty} \left[\binom{n}{k}(1-\gamma)^{n-k}\gamma^k\right]^{1/2} |n-k\rangle\langle n|$$

Channel maps of density operators are trace-preserving and hence deterministic. They are non-selective in the sense that none of the terms in the operator sum are discarded. In the next section, we shall consider the nondeterministic, selective case of trace-decreasing CP maps corresponding to situations that include measurements.

1.4.2 Measurements

A reversible channel map as written in the form of the operator sum in Eq. (1.73) only has one term left in the sum and the one remaining Kraus operator becomes a unitary operator, $\sum_k \hat{A}_k\hat{\rho}\hat{A}_k^\dagger = \hat{U}\hat{\rho}\hat{U}^\dagger$ with $\sum_k \hat{A}_k^\dagger\hat{A}_k = \hat{U}^\dagger\hat{U} = \mathbb{1}$.

Are there also irreversible, non-unitary operations that are described by a map with only one term such that $\hat{\rho} \to \mathcal{E}(\hat{\rho}) = \hat{A}_0\hat{\rho}\hat{A}_0^\dagger$? Since such a non-unitary map must have $\hat{A}_0^\dagger\hat{A}_0 \neq \mathbb{1}$, we would obtain an output density operator with non-unit trace, $\mathrm{Tr}\mathcal{E}(\hat{\rho}) \neq 1$ [see Eq. (1.75)], and the map, in general, would not be trace-preserving. Indeed, the corresponding probabilistic operation could describe, for example, a measurement and the measurement-induced "state reduction" would leave the signal system in a pure, conditional state depending on the measurement result,

$$\frac{\mathcal{E}(\hat{\rho})}{\mathrm{Tr}\mathcal{E}(\hat{\rho})} = \frac{\hat{A}_0\hat{\rho}\hat{A}_0^\dagger}{\mathrm{Tr}(\hat{A}_0^\dagger\hat{A}_0\hat{\rho})} \, . \tag{1.79}$$

Here, the measurement result is labeled by the subscript "0". The state after the measurement is renormalized to unit trace with the unnormalized conditional state divided by the probability for the measurement outcome, $p(k = 0) = \mathrm{Tr}(\hat{A}_0^\dagger\hat{A}_0\hat{\rho}) < 1$. Let us make this probabilistic interpretation in terms of measurement-induced state evolution more plausible.

For this purpose, first we introduce a very useful and well-known extension of the standard von Neumann, projection measurement to a generalized measurement, a so-called *positive-operator valued measure* (POVM). Recall that the measurement of an observable, that is, a Hermitian operator with real eigenvalues, leads to an eigenstate from the observable's orthogonal eigenbasis and the corresponding eigenvalue is the measurement result. This is a projection measurement.

1.4.2.1 POVM

Let us now define the positive operator

$$\hat{E}_k \equiv \hat{A}_k^\dagger\hat{A}_k \, . \tag{1.80}$$

The set of positive operators $\{\hat{E}_k\}$ is referred to as POVM. It determines a set of probabilities given by $p(k) = \mathrm{Tr}(\hat{E}_k\hat{\rho})$. This probability distribution of measurement outcomes should be normalized such that $\sum_k p(k) = \sum_k \mathrm{Tr}(\hat{A}_k^\dagger\hat{A}_k\hat{\rho}) = 1$. This holds for $\sum_k \hat{A}_k^\dagger\hat{A}_k = \mathbb{1}$ and $\mathrm{Tr}\hat{\rho} = 1$. In other words, *any* complete set of positive operators $\{\hat{E}_k\}$ with $\sum_k \hat{E}_k = \mathbb{1}$ defines a generalized measurement. The POVM elements and the Kraus operators coincide if and only if the measurement is a projection measurement so that $\hat{E}_k \equiv \hat{A}_k$, $\hat{A}_k^\dagger = \hat{A}_k$, and $\hat{A}_k\hat{A}_l = \delta_{kl}\hat{A}_k$.

Note that the POVM formalism itself is only about probabilities and not about state evolution. However, we can make statements about non-unitary state evolution as follows.

Consider again the scheme in Figure 1.5. This time, we assume that a projective POVM is applied to the output state of the ancilla after the unitary. This POVM is given by the set of projectors $\{\hat{E}_k\} \equiv \{|k\rangle\langle k|\}$ with an orthonormal basis $\{|k\rangle\}$ for the ancilla system. Similar to what we did before, we can write down the total unitary state evolution of the composite system of signal A and ancilla B, where we assume the ancilla starts in the state $\hat{\rho}_{\mathrm{B}} = |0\rangle_{\mathrm{B}}\langle 0|$. However, this time, we do not simply trace over the ancilla system. Instead, we calculate the probabilities for obtaining the measurement outcome k,

$$\begin{aligned} p(k) &= \mathrm{Tr}_{\mathrm{AB}}\left[\hat{U}_{\mathrm{AB}}\left(\hat{\rho}_{\mathrm{A}} \otimes |0\rangle_{\mathrm{B}}\langle 0|\right)\hat{U}_{\mathrm{AB}}^{\dagger}\left(\mathbb{1}_{\mathrm{A}} \otimes \hat{E}_k\right)\right] \\ &= \mathrm{Tr}_{\mathrm{A}}\left[\sum_l {}_{\mathrm{B}}\langle l|\hat{U}_{\mathrm{AB}}\left(\hat{\rho}_{\mathrm{A}} \otimes |0\rangle_{\mathrm{B}}\langle 0|\right)\hat{U}_{\mathrm{AB}}^{\dagger}\left(\mathbb{1}_{\mathrm{A}} \otimes |k\rangle_{\mathrm{B}}\langle k|\right)|l\rangle_{\mathrm{B}}\right] \\ &= \mathrm{Tr}_{\mathrm{A}}\left(\hat{A}_k\hat{\rho}_{\mathrm{A}}\hat{A}_k^{\dagger}\right) = \mathrm{Tr}_{\mathrm{A}}\left(\hat{A}_k^{\dagger}\hat{A}_k\hat{\rho}_{\mathrm{A}}\right), \end{aligned} \tag{1.81}$$

using $\hat{A}_k \equiv {}_{\mathrm{B}}\langle k|\hat{U}_{\mathrm{AB}}|0\rangle_{\mathrm{B}}$ as before and ${}_{\mathrm{B}}\langle k|l\rangle_{\mathrm{B}} = \delta_{kl}$. This defines the POVM $\{\hat{A}_k^{\dagger}\hat{A}_k\}$ on the signal system $\hat{\rho}_{\mathrm{A}}$. An additional new POVM, $\{\hat{F}_l\}$, acting upon the signal output state would result in the joint probabilities

$$\begin{aligned} p(k,l) &= \mathrm{Tr}_{\mathrm{AB}}\left[\hat{U}_{\mathrm{AB}}\left(\hat{\rho}_{\mathrm{A}} \otimes |0\rangle_{\mathrm{B}}\langle 0|\right)\hat{U}_{\mathrm{AB}}^{\dagger}\left(\hat{F}_l \otimes \hat{E}_k\right)\right] \\ &= \mathrm{Tr}_{\mathrm{A}}\left(\hat{A}_k\hat{\rho}_{\mathrm{A}}\hat{A}_k^{\dagger}\hat{F}_l\right). \end{aligned} \tag{1.82}$$

From this, we can immediately infer the probabilities for obtaining the POVM element $\hat{F}_l$ when the initial state prior to the second POVM is $\hat{\rho}_{\mathrm{A}}^{(k)}$, namely, $\mathrm{Tr}_{\mathrm{A}}[\hat{\rho}_{\mathrm{A}}^{(k)}\hat{F}_l] = p(l|k) = p(k,l)/p(k) = \mathrm{Tr}_{\mathrm{A}}\{[\hat{A}_k\hat{\rho}_{\mathrm{A}}\hat{A}_k^{\dagger}/p(k)]\hat{F}_l\}$. Thus, we must have the conditional state of the first POVM,

$$\hat{\rho}_{\mathrm{A}}^{(k)} = \frac{\hat{A}_k\hat{\rho}_{\mathrm{A}}\hat{A}_k^{\dagger}}{p(k)} = \frac{\hat{A}_k\hat{\rho}_{\mathrm{A}}\hat{A}_k^{\dagger}}{\mathrm{Tr}_{\mathrm{A}}\left(\hat{A}_k^{\dagger}\hat{A}_k\hat{\rho}_{\mathrm{A}}\right)} \equiv \frac{\mathcal{E}(\hat{\rho}_{\mathrm{A}})}{\mathrm{Tr}_{\mathrm{A}}\mathcal{E}(\hat{\rho}_{\mathrm{A}})}. \tag{1.83}$$

Thus, the a-priori-state of the second POVM gives us the a-posteriori-state of the first POVM and hence the state evolution consistent with the first measurement. Here, the a-posteriori-state is pure (provided $\hat{\rho}_{\mathrm{A}}$ is pure), as we have assumed perfect knowledge about the outcome k. More generally, a CP trace-decreasing (CPTD) map can be written in the same way as Eq. (1.73), but with $\sum_k \hat{A}_k^{\dagger}\hat{A}_k < \mathbb{1}$. This may lead to an unpure output state, but the trace is strictly decreasing, provided some information is gained through the measurement. In the special case when no information is gained or, equivalently, when the average is taken over all possible outcomes k, we obtain the ensemble output state,

$$\begin{aligned} \hat{\rho}_{\mathrm{A}}' &= \sum_k p(k)\hat{\rho}_{\mathrm{A}}^{(k)} = \sum_k p(k)\hat{A}_k\hat{\rho}_{\mathrm{A}}\hat{A}_k^{\dagger}/p(k) \\ &= \sum_k \hat{A}_k\hat{\rho}_{\mathrm{A}}\hat{A}_k^{\dagger} = \mathcal{E}(\hat{\rho}_{\mathrm{A}}). \end{aligned} \tag{1.84}$$

This is again a CPTP map and we see that there is a physical interpretation of such a CPTP map. We can think of a channel as an ancilla system like the signal's environment which is monitoring the signal system with random outcomes k. As long as we do not have access to these outcomes, we cannot use them for processing. Therefore, effectively, the input state $\hat{\rho}_{\mathrm{A}}$ is randomly replaced by $\hat{\rho}_{\mathrm{A}}^{(k)}$ with probability $p(k)$. The ensemble state is then the same as before when we traced over the environment using a complete, orthonormal basis.

To summarize, a channel is a CPTP map that *non-selectively* and *deterministically* transforms density operators. It will always map pure states to mixed states, unless it is a unitary channel. A CPTD map is then expressed by a *selective* and hence *nondeterministic* Kraus evolution. It can map pure states to either pure or mixed states, depending, for example, on the resolution of a measurement.

Finally, we shall discuss that there is an alternate way to formulate a generalized measurement besides attaching an ancilla and considering measurements in the product Hilbert space of signal and ancilla, as depicted in Figure 1.5.

1.4.2.2 **Naimark Extension**

Though maybe less physically motivated, but mathematically more systematic, the alternate approach uses an extended Hilbert space from the original signal space corresponding to the total Hilbert space $\mathcal{H} = \mathcal{K} \oplus \mathcal{K}^{\perp}$. Through this direct-sum structure, the POVM is then described by a projection measurement onto the orthogonal set of vectors in the total space,

$$|w_\mu\rangle = |u_\mu\rangle + |N_\mu\rangle \,, \tag{1.85}$$

with $\langle w_\mu | w_\nu \rangle = \delta_{\mu\nu}$. The vectors $\{|u_\mu\rangle\}$ are unnormalized, possibly non-orthogonal state vectors in the Hilbert space $\mathcal{K}$. We may write

$$\hat{E}_\mu = |u_\mu\rangle\langle u_\mu| \,. \tag{1.86}$$

These are the POVM operators of an N-valued POVM with $\sum_{\mu=1}^{N} \hat{E}_\mu = \mathbb{1}$. The vectors $\{|N_\mu\rangle\}$ are defined in the complementary space $\mathcal{K}^{\perp}$ orthogonal to $\mathcal{K}$, with the total Hilbert space $\mathcal{H} = \mathcal{K} \oplus \mathcal{K}^{\perp}$. If the dimension of the signal space is n, with $|u_\mu\rangle = \sum_{i=1}^{n} b_{\mu i} |v_i\rangle$, some complex coefficients $b_{\mu i}$, and $\{|v_i\rangle\}_{i=1}^{n}$ as a basis in $\mathcal{K}$, we have $|N_\mu\rangle = \sum_{i=n+1}^{N} b_{\mu i} |v_i\rangle$ with some complex coefficients $b_{\mu i}$, and $\{|v_i\rangle\}_{i=n+1}^{N}$ as a basis in $\mathcal{K}^{\perp}$. The vectors $\{|N_\mu\rangle\}$ are referred to as a *Naimark extension*.

Let us give an example for a POVM on a single qubit, $n = 2$. Consider a pair of pure and non-orthogonal qubit states,[20]

$$|\chi_\pm\rangle = \alpha|\bar{0}\rangle \pm \beta|\bar{1}\rangle \,, \tag{1.87}$$

where $\alpha > \beta$ are assumed to be real and $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ are two basis states. When we are given a single copy of this qubit without knowing whether it is in the + or the −

[20] Actually, any pair of pure states can be written this way up to a global phase. We use the notation $|\bar{0}\rangle$ and so on in order to indicate that the basis states here are logical basis states. Later, in the optical context, a logical basis state may be encoded into photonic states of several optical modes.

state, there are various restrictions. We cannot perfectly discriminate the two states and so we cannot unambiguously *and* deterministically decide in which quantum state the qubit exists. In fact, if we were able to achieve perfect state discrimination, we could also create more copies from a single copy of the unknown quantum state, thus violating the no-cloning theorem; as a result, we could even communicate at a speed faster than light (recall Section 1.1). The fundamental inability of perfect state discrimination for non-orthogonal states is also the essence of quantum key distribution (see Section 1.7).

However, there are measurement schemes that do achieve state discrimination to some extent in an imperfect fashion, either unambiguously *or* deterministically, or somewhere in between. The two extreme cases are the deterministic discrimination with an ideally minimal error (so-called minimum error discrimination, MED) and the error-free discrimination with an ideally minimal probability for obtaining an inconclusive result (so-called unambiguous state discrimination, USD). In either case, the optimal performance can be derived from the laws of quantum theory.

Now let us consider the USD for the two states in Eq. (1.87). The POVM for this USD may have three elements, $N = 3$, two of which correspond to an error-free identification of the $+$ and $-$ states. The third POVM element would express an additional inconclusive measurement outcome. Thus, we have $\sum_{\mu=1}^{3} \hat{E}_\mu = \mathbb{1}$ with $\hat{E}_\mu$ from Eq. (1.86). The elements $\hat{E}_1$ and $\hat{E}_2$ are conclusive, while $\hat{E}_3$ is inconclusive. Now, in order to make the first two POVM elements unambiguous, that is, error-free, we must satisfy $p(1|-) = \mathrm{Tr}(\hat{E}_1|\chi_-\rangle\langle\chi_-|) = p(2|+) = \mathrm{Tr}(\hat{E}_2|\chi_+\rangle\langle\chi_+|) = 0$, where $p(1|-)$ and $p(2|+)$ are the probabilities for obtaining the 1 outcome for the $-$ state and the 2 outcome for the $+$ state, respectively. Using the ansatz in Eq. (1.85), a projection onto a three-dimensional basis $\{|w_\mu\rangle\}$ can be constructed that satisfies the above constraints. More precisely, the choice of

$$\begin{aligned} |u_{1/2}\rangle &= \frac{1}{\sqrt{2}}\left(\frac{\beta}{\alpha}|\bar{0}\rangle \pm |\bar{1}\rangle\right), \qquad |N_{1/2}\rangle = \frac{1}{\sqrt{2}}\sqrt{1-\frac{\beta^2}{\alpha^2}}|\bar{2}\rangle\,, \\ |u_3\rangle &= \sqrt{1-\frac{\beta^2}{\alpha^2}}|\bar{0}\rangle\,, \qquad |N_3\rangle = -\frac{\beta}{\alpha}|\bar{2}\rangle\,, \end{aligned} \tag{1.88}$$

with $\langle\bar{2}|\bar{0}\rangle = \langle\bar{2}|\bar{1}\rangle = 0$, would even achieve the optimal USD with minimal failure probability, that is, minimal probability for obtaining an inconclusive result, $\mathrm{Prob}_{\mathrm{fail}} = |\langle\chi_+|\chi_-\rangle|$ for equal a priori probabilities [30–32]. The optimality is easily confirmed through

$$\begin{aligned} \mathrm{Prob}_{\mathrm{succ}} &= \mathrm{Tr}\left(\hat{E}_1|\chi_+\rangle\langle\chi_+|\right)/2 + \mathrm{Tr}\left(\hat{E}_2|\chi_-\rangle\langle\chi_-|\right)/2 \\ &= 1 - \mathrm{Prob}_{\mathrm{fail}} \\ &= 1 - \mathrm{Tr}\left(\hat{E}_3|\chi_+\rangle\langle\chi_+|\right)/2 - \mathrm{Tr}\left(\hat{E}_3|\chi_-\rangle\langle\chi_-|\right)/2 \\ &= 1 - (\alpha^2 - \beta^2) = 1 - |\langle\chi_+|\chi_-\rangle| = 2\beta^2\,. \end{aligned} \tag{1.89}$$

The factors 1/2 in lines one and three are the a priori probabilities. Examples of projection measurements, POVMs, and USD on optically encoded quantum states, both in the DV qubit and the CV qumode regime, will be presented in Chapter 2. Such quantum measurements are highly relevant for many applications in optical quantum information, especially quantum communication.

Irreversible quantum operations, measurements

generalized measurement, positive-operator valued measure (POVM):

$$\hat{E}_k = \hat{A}_k^\dagger \hat{A}_k \quad \text{with} \quad \sum_k \hat{E}_k = \mathbb{1} \quad \text{and} \quad \text{probabilities } p(k) = \mathrm{Tr}\left(\hat{E}_k \hat{\rho}\right)$$

non-unitary state evolution, completely positive trace-decreasing (CPTD):

$$\hat{\rho} \to \frac{\mathcal{E}(\hat{\rho})}{\mathrm{Tr}\mathcal{E}(\hat{\rho})} = \frac{\sum_k \hat{A}_k \hat{\rho} \hat{A}_k^\dagger}{\mathrm{Tr}\left(\sum_k \hat{A}_k^\dagger \hat{A}_k \hat{\rho}\right)} \quad \text{with} \quad \sum_k \hat{A}_k^\dagger \hat{A}_k < \mathbb{1}$$

Besides those POVMs on a single qubit or qumode, an important extension are collective, joint POVMs on many qubits or qumodes. An example is the projection onto an entangled-state basis as needed for quantum teleportation. We shall now proceed with an introduction to the notion of entanglement.

1.5 Entanglement

In this section, we will first introduce pure entangled states, focusing on qubit and qumode states. Further, extending the discussion on quantum states for a single qubit and a single qumode in Section 1.2, we shall now look at bipartite qubit and qumode states from a point of view that is based on stabilizers (see the discussion and the box in Section 1.9). For the case of qumodes, the stabilizer states introduced in this section are idealized, unphysical states. We will briefly introduce inseparability criteria for mixed states and entanglement witnesses as well as a few entanglement measures.

1.5.1 Pure States

For any *pure state of two parties*, for instance, a pure state of two qubits or two qumodes, there is always an orthonormal basis for each subsystem, $\{|u_n\rangle\}$ and $\{|v_n\rangle\}$, such that the total state vector can be written in the “Schmidt decomposition” [33] as

$$|\psi\rangle = \sum_n c_n |u_n\rangle |v_n\rangle \ . \tag{1.90}$$

The summation goes over the smaller of the dimensionalities of the two subsystems and would go to infinity for two qumodes. Therefore, for two qubits, there are, in general, two terms. In order to write a bipartite pure state of a qubit and a qumode, two terms are enough as well (see the notion of hybrid entanglement introduced in Chapter 8).

The Schmidt coefficients c_n are real and non-negative, and satisfy $\sum_n c_n^2 = 1$. The Schmidt decomposition may be obtained by writing an arbitrary pure bipartite state as

$$\begin{aligned} |\psi\rangle &= \sum_{mk} a_{mk}|m\rangle|k\rangle = \sum_{nmk} u_{mn}c_{nn}v_{kn}|m\rangle|k\rangle \\ &= \sum_n c_n|u_n\rangle|v_n\rangle \,, \end{aligned} \tag{1.91}$$

with $c_{nn} \equiv c_n$. In the first step, the matrix a with complex elements a_{mk} is diagonalized using singular-value decomposition, $a = ucv^{\mathrm{T}}$, where u and v are unitary matrices and c is a diagonal matrix with real, non-negative elements. In the second step, we defined $|u_n\rangle \equiv \sum_m u_{mn}|m\rangle$ and $|v_n\rangle \equiv \sum_k v_{kn}|k\rangle$ which form orthonormal sets due to the unitarity of u and v, and the orthonormality of $|m\rangle$ and $|k\rangle$.

A pure state of two finite-dimensional, d-level systems is maximally entangled when the Schmidt coefficients of the total state vector are all equal. Since the eigenvalues of the reduced density operator after tracing out one half of a bipartite state are the Schmidt coefficients squared,

$$\hat{\rho}_1 = \mathrm{Tr}_2\hat{\rho}_{12} = \mathrm{Tr}_2|\psi\rangle_{12}\langle\psi| = \sum_n c_n^2|u_n\rangle_1\langle u_n| \,, \tag{1.92}$$

tracing out either subsystem of a maximally entangled state leaves the other half in the maximally mixed state $\mathbb{1}/d$. In other words, if one party is discarded, the remaining party is in a maximally noisy state with maximum entropy. Conversely, a pure bipartite state is factorizable (not entangled) if and only if the number of nonzero Schmidt coefficients, the so-called *Schmidt rank*, is one. In this case, the reduced states are pure and have zero entropy.

A unique measure of bipartite entanglement for pure states is given by the partial von Neumann entropy, that is, the von Neumann entropy as defined in Eq. (1.22) for the remaining system after tracing out either subsystem [34], $-\mathrm{Tr}\hat{\rho}_1 \log_d \hat{\rho}_1 = -\mathrm{Tr}\hat{\rho}_2 \log_d \hat{\rho}_2 = -\sum_n c_n^2 \log_d c_n^2$, with $\mathrm{Tr}_2\hat{\rho}_{12} = \hat{\rho}_1$, $\mathrm{Tr}_1\hat{\rho}_{12} = \hat{\rho}_2$. This measure ranges between zero and one, and for qubits ($d = 2$) its units are "ebits". It can be understood as the amount of maximum entanglement contained in a given pure state.[21] For example, an entropy of 0.4 means that asymptotically 1000 copies of the state can be transformed into 400 maximally entangled states through deterministic state transformations using local operations and classical communication [5].

[21] For general bipartite qumode states, there are some complications of this entanglement entropy. The entropy fails to be continuous in the sense that there are (rather artificial) states that have arbitrarily large entanglement, though being arbitrarily close to a pure product state. However, through restriction on bounded mean energies continuity of the entanglement can be recovered [35].

1.5.1.1 Qubits

For two qubits, a maximally entangled basis is given by the four "Bell states",[22]

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) , \qquad |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) . \tag{1.93}$$

These are stabilizer states with nonlocal stabilizer generators.[23] For instance, the $|\Phi^{+}\rangle$ state has stabilizer generators $\langle X \otimes X, Z \otimes Z\rangle$ corresponding to a stabilizer group $\{\mathbb{1} \otimes \mathbb{1}, X \otimes X, -Y \otimes Y, Z \otimes Z\}$. Any of these Pauli products has eigenvalue $+1$ when applied upon $|\Phi^{+}\rangle$. The set of generators is sufficient to represent every stabilizer since the products $(X \otimes X)(Z \otimes Z) = XZ \otimes XZ = -Y \otimes Y$ and $(X \otimes X)(X \otimes X) = \mathbb{1} \otimes \mathbb{1}$ must have $+1$ eigenvalue as well.

Recall that a one-qubit stabilizer state has a single stabilizer generator, namely, ± 1 times one of the Pauli operators. The stabilizer group has two elements after adding the unity operator. Two qubits require two stabilizer generators as a minimal set to give a stabilizer group of four elements. For instance, a product state of two qubits, $|0\rangle \otimes |0\rangle$, is a stabilizer state with stabilizer group $\{\mathbb{1} \otimes \mathbb{1}, \mathbb{1} \otimes Z, Z \otimes \mathbb{1}, Z \otimes Z\}$ and, in this case, local stabilizer generators[24] $\langle \mathbb{1} \otimes Z, Z \otimes \mathbb{1}\rangle$. The *nonlocal* stabilizer generators of the four Bell states in Eq. (1.93) are easily found to be

$$\begin{aligned} &\langle X \otimes X, Z \otimes Z\rangle , \qquad &&\langle X \otimes X, -Z \otimes Z\rangle , \\ &\langle -X \otimes X, Z \otimes Z\rangle , \qquad &&\langle -X \otimes X, -Z \otimes Z\rangle , \end{aligned} \tag{1.94}$$

respectively. The two-qubit stabilizer states are either product states or maximally entangled states. The two-qubit non-stabilizer states are the non-maximally (partially) entangled states (or products of non-stabilizer states).

1.5.1.2 Qumodes

Now, consider the case of two qumodes. The "CV Bell states" for two qumodes may be written as

$$|\Psi(u,v)\rangle = \frac{1}{\sqrt{\pi}} \int dx e^{2ixv} |x\rangle |x - u\rangle . \tag{1.95}$$

Although these states obey the completeness and orthogonality relations

$$\begin{aligned} &\int du dv |\Psi(u,v)\rangle\langle\Psi(u,v)| = \mathbb{1} \otimes \mathbb{1} , \\ &\qquad \langle\Psi(u,v)|\Psi(u',v')\rangle = \delta(u - u')\delta(v - v') , \end{aligned} \tag{1.96}$$

they are nonetheless unphysical since they exhibit an infinite degree of quantum correlations. This is similar to the position and momentum eigenstates of a single qumode with infinitely precise position and momentum eigenvalues as depicted in Figure 1.3. Each of the CV Bell states is similarly determined through infinitely

[22] We shall use the notations $|\Phi^{\pm}\rangle$ and $|\Phi^{(\pm)}\rangle$, and so on, interchangeably throughout.

[23] For a definition of stabilizers, see the discussion and the box in Section 1.9.

[24] Where, more precisely, "local" refers to the local subgroup into which the total stabilizer group of the state can be split together with a nonlocal subgroup. The local subgroup then contains stabilizer operators that act exclusively upon either subsystem [36]. For the product state $|0\rangle \otimes |0\rangle$, the whole stabilizer is given by the local subgroup $\{\mathbb{1}, Z\} \cdot \{\mathbb{1}, Z\}$.

precise, continuous eigenvalues. However, for two qumodes, we need two such eigenvalues, corresponding to two *nonlocal* observables with $(\hat{x}_1 - \hat{x}_2)|\Psi(u,v)\rangle = u|\Psi(u,v)\rangle$ and $(\hat{p}_1 + \hat{p}_2)|\Psi(u,v)\rangle = v|\Psi(u,v)\rangle$.

Expressed in terms of the WH shift operators, we can equivalently write for all t, s,

$$\begin{aligned} \mathrm{e}^{-2\mathrm{i}tu}\mathrm{e}^{+2\mathrm{i}t(\hat{x}_1-\hat{x}_2)}|\Psi(u,v)\rangle &= \mathrm{e}^{-2\mathrm{i}tu}Z(t)\otimes Z^\dagger(t)|\Psi(u,v)\rangle \\ &= |\Psi(u,v)\rangle\ , \\ \mathrm{e}^{+2\mathrm{i}sv}\mathrm{e}^{-2\mathrm{i}s(\hat{p}_1+\hat{p}_2)}|\Psi(u,v)\rangle &= \mathrm{e}^{+2\mathrm{i}sv}X(s)\otimes X(s)|\Psi(u,v)\rangle \\ &= |\Psi(u,v)\rangle\ . \end{aligned} \tag{1.97}$$

In other words, for the unphysical, infinitely correlated CV Bell states, we obtain the nonlocal stabilizer generators

$$\langle \mathrm{e}^{+2\mathrm{i}sv}X(s)\otimes X(s), \mathrm{e}^{-2\mathrm{i}tu}Z(t)\otimes Z^\dagger(t)\rangle\ . \tag{1.98}$$

Note that for $v = 0$, this would be a unique representation for the famous two-particle state presented by Einstein, Podolsky, and Rosen (EPR) which is quantum mechanically correlated in the positions ($x_1 - x_2 = u$) and the momenta ($p_1 + p_2 = 0$) [23]. In the optical context, a physical version of the EPR state corresponds to a Gaussian two-mode squeezed state in the limit of large squeezing (see Chapter 3). Moreover, similar to the two-qubit stabilizers, the two-qumode stabilizers here are useful to construct so-called entanglement witnesses. These witnesses would enable one to detect the entanglement of the physical, finitely correlated, and possibly even noisy mixed-state approximations of the EPR state. How to find such witnesses for qubits and qumodes will be discussed in Chapter 3. At this point, we shall proceed by looking at the entanglement of mixed states, inseparability criteria, and the definition of entanglement witnesses.

Given an arbitrary two-party (e.g., two-qubit or two-qumode) density operator, how can we find out whether the bipartite state is entangled or not? For this purpose, first of all, a definition of entanglement is needed which goes beyond that of pure-state entanglement expressed by the Schmidt rank and so is applicable to mixed states as well.

1.5.2 Mixed States and Inseparability Criteria

A *mixed state of two parties* is separable if its total density operator can be written as a mixture (a convex sum) of product states,[25]

$$\hat{\rho}_{12} = \sum_i \eta_i \hat{\rho}_{i,1} \otimes \hat{\rho}_{i,2}\ . \tag{1.99}$$

[25] Corresponding to a *classically correlated* state [37]. For instance, for the qubit or the qumode Bell states, the nonclassical character of entanglement is reflected by the nonlocal stabilizer generators simultaneously in terms of X and Z. However, note that this notion of nonlocality is weaker than the historically well-known notion of nonlocality that refers to the inapplicability of local realistic models. In fact, Werner's [37] original intention was to demonstrate that quantum states exist which are inseparable according to the convex-sum definition and yet admit a local realistic description.

Otherwise, it is inseparable and hence entangled. In general, it is a highly nontrivial question whether a given density operator is separable or inseparable.

A very powerful method to test for inseparability is Peres' *partial transpose* criterion [38]. For a separable state as in Eq. (1.99), transposition of either density matrix yields again a legitimate non-negative density operator with unit trace,

$$\hat{\rho}'_{12} = \sum_i \eta_i (\hat{\rho}_{i,1})^{\mathrm{T}} \otimes \hat{\rho}_{i,2} \tag{1.100}$$

since $(\hat{\rho}_{i,1})^{\mathrm{T}} = (\hat{\rho}_{i,1})^*$ corresponds to a legitimate density matrix. This is a necessary condition for a separable state, and hence a single negative eigenvalue of the partially transposed density matrix is a sufficient condition for inseparability. Applied to one party entangled with another party, transposition may indeed lead to an unphysical state because it is a positive but not a CP map. For inseparable states of two qubits and of one qubit and one qutrit, partial transposition always leads to an unphysical state [39]. The same holds true for any bipartite Gaussian state of one qumode entangled with arbitrarily many other qumodes (see Chapter 3).

1.5.3 Entanglement Witnesses and Measures

Independent of partial transposition, an *entanglement witness* $\hat{W}$ is an observable whose expectation value is non-negative for all separable states $\hat{\rho}_{\mathrm{sep}}$, $\mathrm{Tr}(\hat{W}\hat{\rho}_{\mathrm{sep}}) \geq 0$, and negative for some inseparable state $\hat{\rho}$, $\mathrm{Tr}(\hat{W}\hat{\rho}) < 0$ (see Figure 1.6).

A very important class of entanglement witnesses is given by the Bell-type inequalities imposed by local realistic theories [41]. For both qubits and qumodes, we shall discuss the canonical and most commonly used entanglement witnesses in Chapter 3. These witnesses are independent of local realism. Since the inseparability criteria expressed in terms of expectation values of observables are directly measurable, entanglement witnesses are of great significance for the experimental verification of the presence of entanglement.

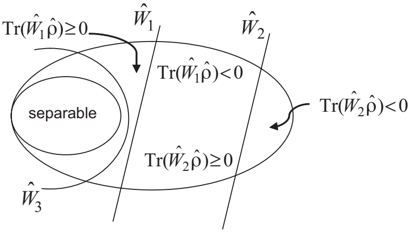
$\mathrm{Tr}(\hat{W}_1\hat{\rho})\geq 0$
$\hat{W}_1$
$\hat{W}_2$
$\mathrm{Tr}(\hat{W}_1\hat{\rho})<0$
separable
$\mathrm{Tr}(\hat{W}_2\hat{\rho})<0$
$\mathrm{Tr}(\hat{W}_2\hat{\rho})\geq 0$
$\hat{W}_3$

Figure 1.6 Entanglement witnesses are Hermitian operators that define hyperplanes in the space of density operators (states), separating some inseparable states from all separable states. The plane closer to the set of separable states represents a "better" witness $\hat{W}_1$ than the other plane corresponding to $\hat{W}_2$, as the former detects more inseparable states. An optimal linear witness would correspond to a plane tangent on the set of separable states. However, there are even better witnesses like $\hat{W}_3$ which are nonlinear and can detect even more inseparable states [40].

Besides those qualitative inseparability criteria, which we may call entanglement *qualifiers*, a more ambitious task is to provide entanglement measures and to obtain entanglement *quantifiers* for a given density operator, both theoretically and experimentally. In general, the known measures for mixed-state entanglement are not unique. In the summary box 'Entanglement', we included some of the most commonly used and most convenient entanglement measures.

In the case of pure states, (most of) these measures would coincide. The naive approach for extending pure-state quantifiers to mixed states would be to simply apply a pure-state measure such as the reduced von Neumann entropy to every term in a density operator decomposition. However, in general, a given decomposition $\sum_k p_k |\psi_k\rangle_{12}\langle\psi_k|$ may then give a completely wrong result,

$$\sum_k p_k S\left[\mathrm{Tr}_2\left(|\psi_k\rangle_{12}\langle\psi_k|\right)\right] . \tag{1.101}$$

For instance, the maximally mixed state of two qubits, $\hat{\rho}_{12} = \mathbb{1}_{12}/4$, can be decomposed as

$$\hat{\rho}_{12} = (|\Phi^+\rangle_{12}\langle\Phi^+| + |\Phi^-\rangle_{12}\langle\Phi^-| + |\Psi^+\rangle_{12}\langle\Psi^+| + |\Psi^-\rangle_{12}\langle\Psi^-|)/4 \tag{1.102}$$

using the two-qubit Bell basis in Eq. (1.93). In this case, every term corresponds to a maximally entangled state with unit reduced entropy. So the average reduced entropy as calculated by Eq. (1.101) also gives one ebit instead of the correct result of zero ebits for a separable density operator written as

$$\begin{aligned}\hat{\rho}_{12} = (&|0\rangle_1\langle 0| \otimes |0\rangle_2\langle 0| + |0\rangle_1\langle 0| \otimes |1\rangle_2\langle 1| \\ &+ |1\rangle_1\langle 1| \otimes |0\rangle_2\langle 0| + |1\rangle_1\langle 1| \otimes |1\rangle_2\langle 1|)/4 .\end{aligned} \tag{1.103}$$

Therefore, for a globally mixed state, we only obtain sensible results if we *minimize* the average reduced entropy over *all possible ensemble decompositions*,

$$E_{\mathrm{F}}(\hat{\rho}_{12}) \equiv \inf_{p_k,\psi_k} \sum_k p_k S\left[\mathrm{Tr}_2\left(|\psi_k\rangle_{12}\langle\psi_k|\right)\right] . \tag{1.104}$$

This is the so-called entanglement of formation. In general, the minimization over all decompositions is hard to compute. However, for two qubits, the entanglement of formation can be obtained through the concurrence [42]. Another important and more practical (i.e., relatively easily computable) mixed-state entanglement quantifier is the logarithmic negativity which is based upon the negativity after partial transposition [43–45].

The logarithmic negativity is defined as follows,

$$E_{\mathrm{N}}(\hat{\rho}_{12}) \equiv \log_2 \left|\left|\hat{\rho}_{12}^{\mathrm{T}_2}\right|\right| , \tag{1.105}$$

where $||\hat{A}|| \equiv \mathrm{Tr}\sqrt{\hat{A}^\dagger \hat{A}}$ is the so-called trace norm and $\hat{\rho}_{12}^{\mathrm{T}_2}$ is the partial transpose of a given bipartite state $\hat{\rho}_{12}$ with respect to subsystem 2. This measure is an entanglement monotone (i.e., it does not increase under local operations and classical communication) and, in addition, it is additive.[26] The trace norm of the partial transpose corresponds to the sum of the modulus of its eigenvalues. For instance, for a two-qubit Bell state $\hat{\rho}_{12}$, we have $||\hat{\rho}_{12}^{\mathrm{T}_2}|| = 2$, as the eigenvalues of $\hat{\rho}_{12}^{\mathrm{T}_2}$ are $\{-1/2, 1/2, 1/2, 1/2\}$. Conversely, for a separable state $\hat{\rho}_{12}$, we always obtain $||\hat{\rho}_{12}^{\mathrm{T}_2}|| = 1$. Thus, the Bell state gives $E_{\mathrm{N}}(\hat{\rho}_{12}) = 1$, whereas a separable state has $E_{\mathrm{N}}(\hat{\rho}_{12}) = 0$. In general, any entanglement measure should be an entanglement monotone and should vanish for separable states.

Entanglement

bipartite pure states: separable iff Schmidt rank is one in Schmidt decomposition $|\psi\rangle_{12} = \sum_n c_n |u_n\rangle_1 |v_n\rangle_2$

bipartite mixed states: separable iff $\hat{\rho}_{12} = \sum_i \eta_i \hat{\rho}_{i,1} \otimes \hat{\rho}_{i,2}$

qualifiers, witnesses: $\forall \hat{\rho}_{\mathrm{sep}} \mathrm{Tr}(\hat{W}\hat{\rho}_{\mathrm{sep}}) \geq 0$ and $\exists \hat{\rho}$ such that $\mathrm{Tr}(\hat{W}\hat{\rho}) < 0$
quantifiers: reduced entropy for pure states: $E(|\psi\rangle_{12}) \equiv S[\mathrm{Tr}_2(|\psi\rangle_{12}\langle\psi|)]$
entanglement of formation: $E_{\mathrm{F}}(\hat{\rho}_{12}) \equiv \inf_{\rho_k, \psi_k} \sum_k \rho_k S[\mathrm{Tr}_2(|\psi_k\rangle_{12}\langle\psi_k|)]$
logarithmic negativity: $E_{\mathrm{N}}(\hat{\rho}_{12}) \equiv \log_2 ||\hat{\rho}_{12}^{\mathrm{T}_2}||$

⊙ **Qubits:** maximally entangled two-qubit Bell states:

$$|\Phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}, \quad |\Psi^{\pm}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$$

stabilized by

$$\langle X \otimes X, Z \otimes Z\rangle, \langle X \otimes X, -Z \otimes Z\rangle, \langle -X \otimes X, Z \otimes Z\rangle, \langle -X \otimes X, -Z \otimes Z\rangle$$

〰 **Qumodes:** maximally entangled two-qumode Bell states:

$$|\Psi(u,v)\rangle = \int \mathrm{d}x \mathrm{e}^{2\mathrm{i}xv} |x\rangle |x-u\rangle / \sqrt{\pi}$$

stabilized by

$$\langle \mathrm{e}^{+2\mathrm{i}sv} X(s) \otimes X(s), \mathrm{e}^{-2\mathrm{i}tu} Z(t) \otimes Z^{\dagger}(t)\rangle$$

Since the trace norm of the partial transpose effectively expresses to what extent $\hat{\rho}_{12}^{\mathrm{T}_2}$ fails to represent a physical state, it can be considered a quantitative version of the above qualitative partial transpose criterion.

This connection is easier to understand by looking at the so-called negativity, defined as $N(\hat{\rho}_{12}) \equiv (||\hat{\rho}_{12}^{\mathrm{T}_2}|| - 1)/2$. This quantity corresponds to the modulus of the sum of the *negative* eigenvalues of $\hat{\rho}_{12}^{\mathrm{T}_2}$, and becomes $N(\hat{\rho}_{12}) = 1/2$ for a two-qubit Bell state and $N(\hat{\rho}_{12}) = 0$ for any separable state. In this sense, $N(\hat{\rho}_{12})$ is the

[26] However, it is not convex, and, as an exception to what we said before, it does not reduce to the entanglement entropy for all pure states.

actual measure of negativity. However, though also being an entanglement monotone, $N(\hat{\rho}_{12})$ fails to be additive. Therefore, usually, the logarithmic negativity is preferred.

A discussion of *multipartite* entangled states of many qubits or qumodes will be postponed until Chapter 3. Such a generalization is important in order to define and investigate qubit/qumode cluster and graph states.

1.6 Quantum Teleportation

Quantum teleportation [17] is the reliable transfer of quantum information through a classical communication channel using shared entanglement. It works as follows (see Figure 1.7). After an entangled state is generated and distributed between two parties, an external system in an arbitrary, even completely unknown quantum state is jointly measured together with one half of the entangled state. Finally, when the measurement result is received at the other half of the entangled state, this half is transformed by a basic operation (such as a bit or phase flip for qubits or a phase-space displacement for qumodes) conditioned upon the measurement outcome.

When we think of entanglement as the universal resource for quantum information processing, we may refer to quantum teleportation as the fundamental quantum information protocol or subroutine. Quantum teleportation of *states* (as introduced here and discussed in more detail in Chapter 4) has applications in quantum communication (see the following section) as well as quantum computation. In the latter case, it would enable one, in principle, to connect different quantum computers when every quantum computer performs only a part of the whole computation.

Besides transferring quantum information between quantum computers and propagating it through quantum computers, there is an extended version of quantum teleportation which incorporates a controlled unitary evolution of quantum information into the teleportation protocol. This is quantum teleportation of *gates* and using such gate teleportations for computation corresponds to a certain realization of measurement-based quantum computation (see Chapter 6). The measurements in this case are projections onto an entangled basis and so they are not always easy to implement, for example, in an optical approach. Complete state transfer or evolution is also possible by performing the corresponding entangling operations offline with only local projection measurements performed online (see Chapter 7).

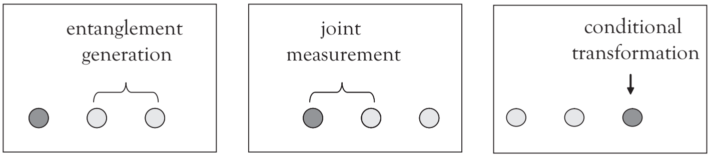

Figure 1.7 The fundamental protocol of quantum teleportation.

1.6.1 Discrete Variables

Let us consider quantum teleportation in finite dimensions. How the original DV quantum teleportation protocol [17] works can be understood from the following decomposition,

$$|\phi\rangle_{\text{in}} \otimes |\Psi_{0,0}\rangle_{12} = \frac{1}{d} \sum_{\alpha,\beta=0}^{d-1} |\Psi_{\alpha,\beta}\rangle_{\text{in},1}\, \hat{U}_2^{\dagger}(\alpha,\beta)|\phi\rangle_2 \,. \tag{1.106}$$

Here, we use α and β as discrete indices. The initial total state vector is a product of an arbitrary quantum state $|\phi\rangle_{\text{in}}$ for the input qudit (d-level system) and a particular maximally entangled state $|\Psi_{0,0}\rangle_{12}$ for qudits 1 and 2 (see below). A projection measurement of the input qudit and qudit one onto the maximally entangled basis of "qudit Bell states",

$$|\Psi_{\alpha,\beta}\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \exp(2\pi \mathrm{i} k\beta/d)|k\rangle|k \oplus \alpha\rangle \,, \tag{1.107}$$

reduces the above decomposition according to the measurement result (α_0, β_0). The qudit Bell states are complete and orthonormal,

$$\sum_{\alpha,\beta=0}^{d-1} |\Psi_{\alpha,\beta}\rangle\langle\Psi_{\alpha,\beta}| = \mathbb{1} \otimes \mathbb{1} \,, \quad \langle\Psi_{\alpha,\beta}|\Psi_{\alpha',\beta'}\rangle = \delta_{\alpha\alpha'}\delta_{\beta\beta'} \,. \tag{1.108}$$

Finally, applying to qudit two the unitary transformation that corresponds to the Bell measurement result (α_0, β_0) will correct the remaining $\hat{U}_2^{\dagger}(\alpha_0, \beta_0)$ operation in Eq. (1.106) and transform qudit two to the input state (the initial state of qudit "in"). The unitary transformations are defined as

$$\hat{U}(\alpha,\beta) = \sum_{k=0}^{d-1} \exp(2\pi \mathrm{i} k\beta/d)|k\rangle\langle k \oplus \alpha| \,, \tag{1.109}$$

and $\oplus$ means addition modulo d.

Quantum teleportation of an arbitrary quantum state from qudit "in" to qudit two is, in principle, independent of any spatial limitations. Suppose the two parties Alice and Bob initially share the maximally entangled state of qudits one and two. Alice is then capable of transferring an arbitrary quantum state from her location to Bob's. All she has to do is jointly measure the qudits "in" and one ("Bell measurement") and convey the measurement result to Bob through a classical communication channel. Finally, Bob has to apply the corresponding unitary transformation to qudit two. There are now three aspects of quantum teleportation that are particularly worth pointing out:

1. An unknown input state remains unknown to both Alice and Bob throughout the entire teleportation process. If Alice did gain some information through her

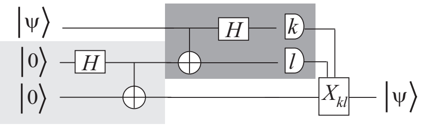

Figure 1.8 A quantum circuit description of qubit quantum teleportation. The part of the circuit in the light gray box is for entanglement generation between the two ancilla qubits. The part in the dark gray box is the circuit for the Bell measurement of the signal state and one half of the entangled pair.

Bell measurement, Bob would no longer obtain a perfect replica of the input state.

2. The input system does not remain in its initial state because of the Bell measurement. This fact ensures that no-cloning is not violated.
3. A contradiction to special relativity is avoided because the classical communication required between Alice and Bob is restricted by the speed of light.

For qubits ($d = 2$), the maximally entangled states $|\Psi_{\alpha,\beta}\rangle$ become the four Bell states from Eq. (1.93). The unitary transformations in this case correspond to the identity operator, $\hat{U}(0,0) = |0\rangle\langle 0| + |1\rangle\langle 1| = \mathbb{1}$, and the three Pauli operators

$$\begin{aligned}\hat{U}(1,0) &= |0\rangle\langle 1| + |1\rangle\langle 0| = X\ ,\\ \hat{U}(1,1) &= |0\rangle\langle 1| - |1\rangle\langle 0| = \mathrm{i}Y\ ,\\ \hat{U}(0,1) &= |0\rangle\langle 0| - |1\rangle\langle 1| = Z\ .\end{aligned} \tag{1.110}$$

Therefore, Bob will accomplish quantum teleporation of the input qubit by either flipping his qubit (X), flipping its phase (Z), doing both (Y), or doing nothing ($\mathbb{1}$). A quantum circuit description of qubit quantum teleportation is shown in Figure 1.8. The Bell measurement circuit is the inverse of the entanglement generation circuit, each consisting of Hadamard and CNOT gates (both belonging to the Clifford group of qubit unitaries, see Sections 1.3 and 1.8).

1.6.2 Continuous Variables

The translation of the quantum circuit for quantum teleportation from qubits to qumodes is straightforward. For this purpose, we need to replace the qubit gates by their qumode analogues, that is, the Hadamard gate by the Fourier gate and the two-qubit CNOT gate by a corresponding two-qumode entangling gate. We postpone the details about such gate sets until Section 1.8. However, we should mention that the two-qumode entangling gate can be effectively achieved through a linear beam splitter transformation (see Chapters 2 and 4). As a consequence, both the entanglement generation and the Bell measurement circuit become highly accessible to optical implementations when one-qumode stabilizer states and one-qumode projection measurements onto stabilizer states are available (and these are available in the form of squeezed states and homodyne detections, see Chapters 2 and 4). In this sense, quantum teleportation also serves as the prime example to reveal the practical significance of the CV approaches.

In order to illustrate the analogy between the above protocol for finite-dimensional, DV quantum teleportation and that for infinite-dimensional, CV quantum teleportation, we may write the following decomposition for the CV case,

$$|\phi\rangle_{\text{in}} \otimes |\Psi(0,0)\rangle_{12} = \frac{1}{\pi} \int \mathrm{d}u\mathrm{d}v |\Psi(u,v)\rangle_{\text{in},1} \hat{U}_2^\dagger(u,v)|\phi\rangle_2 \,, \tag{1.111}$$

with the CV Bell states of Eq. (1.95) and the unitary transformations,

$$\hat{U}(u,v) = \int \mathrm{d}x \mathrm{e}^{2\mathrm{i}xv} |x\rangle\langle x-u| \,. \tag{1.112}$$

These unitaries are equivalent to WH shifts expressed by $X(u)$ and $Z(v)$. The CV protocol is then completely analogous to the DV case, except that the entangled state used in the CV case is an unphysical, unnormalizable state. Only with this idealization do we obtain perfect quantum state transfer similar to the qubit case, with no information gain by Alice through her Bell measurement.

In a physical qumode quantum teleportation protocol using properly normalized, finite-energy states, Alice does gain partial information and the quantum state transfer to Bob becomes imperfect. This will be one of the subjects of Chapter 4, including the discussion of several variations of optical CV quantum teleportation experiments.

1.7 Quantum Communication

The goal of quantum communication is the reliable transfer of arbitrary quantum states (drawn from an alphabet of states) between a sender, usually named Alice, and a receiver, Bob. More colloquially, we can say that quantum communication is "the art to transfer quantum states" [46]. This may then lead to various applications, some of which are already emerging as an existing technology such as the secure distribution of a classical key through quantum key distribution (QKD) [47–49]. Other applications appear farther away from realization such as the connection of spatially separated quantum computers for distributed quantum computing and a kind of quantum internet [50].

Related with the above concepts and applications are the following important lines of current research efforts:

- search for practical QKD protocols,
- security proofs for unconditionally secure QKD,
- long-distance quantum communication beyond 200 km.

Another, more traditional branch of quantum communication deals with the fundamental limits that quantum theory imposes on classical communication. We

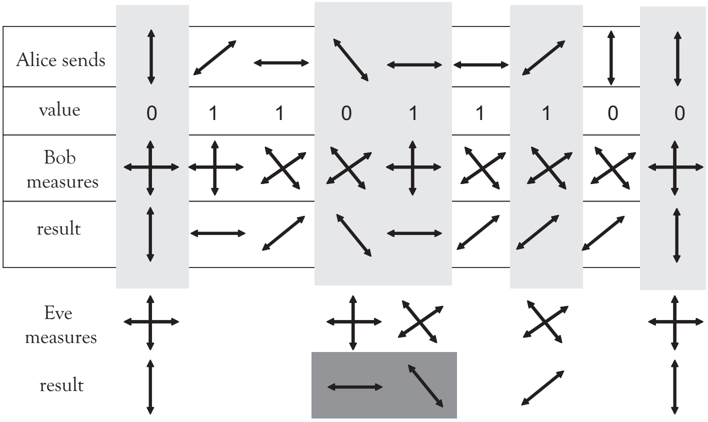

Figure 1.9 The concept of quantum key distribution [18]. Alice randomly prepares states from two non-orthogonal bases, for instance, corresponding to the qubit stabilizer states $\pm Z$ and $\pm X$, where the sign denotes the bit value 0 or 1. Bob, after receiving the states from Alice, randomly performs measurements in either basis. By postselecting those events where the bases coincide, correlated data between Alice and Bob will be obtained. In the presence of Eve, on average 25% of those otherwise correlated data would contain errors which can be detected by Alice and Bob on a subsample of their data.

shall get back to this quantum extension of classical information theory at the end of this section. The more recent approaches to quantum communication aim at the exploitation of nonclassical quantum features such as non-orthogonality and entanglement for quantum-enhanced communication. Let us briefly discuss the concepts behind QKD as an example.

1.7.1 Key Distribution

Quantum key distribution (QKD) [18, 20, 51] allows, in principle, for unconditionally secure communication. It relies upon the inability of a potential eavesdropper (“Eve”) to discriminate non-orthogonal quantum states. Recall that Eve would be able to perfectly distinguish non-orthogonal states if she was able to produce copies of such states (Section 1.1). So no-cloning is a necessary requirement for quantum cryptography, and while perfect quantum cloning would prevent secure QKD, an approximate cloning attack performed by Eve may still be a threat to the security of a realistic QKD protocol, including imperfect channel transmissions.

In the BB84 protocol [18], Alice randomly prepares states from two non-orthogonal bases, for instance, corresponding to the qubit stabilizer states $\pm Z$ and $\pm X$ where the sign denotes the bit value zero or one (see Figure 1.9). Bob, after receiving the states from Alice, randomly performs measurements in either basis. By postselecting only those events where the bases coincide, correlated data between Alice and Bob will be obtained.

Now, Eve may, prior to Bob's measurements, intercept the communication between Alice and Bob and randomly pick her own basis in order to retrieve Alice's key values. However, only in half of the cases would Eve's basis coincide with that of Alice. As a consequence for those events where Eve's basis choice is wrong, she would have to pass on a state to Bob for which he obtains a bit value differing from Alice's bit value in half of the cases. Therefore, in this scenario, 25% of those otherwise correlated data would become contaminated with errors. Whenever Alice and Bob detect such a high error rate for a subsample of their data, they would abandon their protocol and start from scratch. More generally, the tolerable error rate depends on the quality of the quantum channel between Alice and Bob, and on the most general quantum operations that are available to Eve.

Note that in order to prevent Eve from pretending to be Bob and so from eventually sharing the key herself with Alice, Alice and Bob need to start with an initially shared key in order to utilize classical authentication techniques. The QKD protocol will then enable them to grow a larger key. Finally, they can use a sufficiently large key to exchange a message employing the well-known one-time pad.

The BB84 protocol as described so far is a so-called *prepare-and-measure* scheme. It does not directly depend on the physical distribution of entangled states; it relies upon preparing and measuring non-orthogonal quantum states. In fact, just any two non-orthogonal quantum states would suffice to do QKD [51]. As a consequence, instead of qubit states, qumode states may serve as well as a carrier for QKD. Especially, coherent states of light (see Chapter 2), forming an overcomplete, non-orthogonal set represent a convenient choice with regards to practical implementations. A scheme based on coherent states was already implemented experimentally [52].

In an *entanglement-based* QKD protocol [20], Alice and Bob would attempt to generate correlated data by distributing and measuring entangled pairs. In this case, one has to assume that Eve has total control over the whole three-party system – effectively an arbitrarily powerful Eve may distribute any tripartite state (see Chapter 3) among Alice, Bob, and herself. Now, whenever tracing over Eve's system (mimicking the situation where Eve corresponds to an untrusted, non-cooperating third part or the inaccessible environmental degrees of freedom of an imperfect channel) leads to a separable state between Alice and Bob, they can no longer establish a secure key [19]. The reason for this is that the so-called intrinsic information (see later Section 1.7.3 for some words on classical information measures) for Alice and Bob provides an upper bound on the secure key rate [53] and it would strictly vanish for a separable, reduced state of Alice and Bob.

A conceptually very important observation now is that any prepare-and-measure scheme can also be rephrased such that the measured data for Alice and Bob (given by a joint probability distribution for their POVMs) can be used as a secure key provided that these data are inconsistent with a separable state for Alice and Bob [19]. The additional step for proving this is that in this case, the reduced density operator for Alice alone is known and controlled by Alice. It is basically given by the trace over a bipartite source state of the form,

$$|\chi\rangle_{\mathrm{AB}} = \sum_i \sqrt{p_i}|u_i\rangle_{\mathrm{A}} \otimes |\psi_i\rangle_{\mathrm{B}} \ , \tag{1.113}$$

with an orthonormal basis $\{|u_i\rangle\}$ and a non-orthogonal set of states $\{|\psi_i\rangle\}$ [54]. By measuring in the basis $\{|u_i\rangle\}$, Alice effectively prepares the non-orthogonal signal states $\{|\psi_i\rangle\}$, for instance, the BB84 states stabilized by $\pm Z$ and $\pm X$. However, still, when Eve has access to Bob's system, a reduced state for Alice and Bob which is separable leads to a vanishing intrinsic information and so no secure key is available.

The bottom line is that in any secure QKD protocol, Alice and Bob must share data that cannot be interpreted as coming from a separable state – the data have to come from an *effectively entangled* state.

When a certain alphabet of qumode states is used for QKD, for instance, the two non-orthogonal qumode states $|\psi_0\rangle$ and $|\psi_1\rangle$, the interpretation of the corresponding prepare-and-measure scheme in terms of effective entanglement leads to a very special manifestation of entanglement, namely, that between a qubit and a qumode in a kind of hybrid entangled state, $(|u_0\rangle_{\mathrm{A}} \otimes |\psi_0\rangle_{\mathrm{B}} + |u_1\rangle_{\mathrm{A}} \otimes |\psi_1\rangle_{\mathrm{B}})/\sqrt{2}$. We shall get back to this notion of hybrid entanglement in Chapter 8. Further, it is useful to realize that the necessary precondition for secure QKD according to the theorem of [19], namely, the presence of (effective) entanglement, can be satisfied in the CV setting, in principle, for any channel losses: CV qumode entangled states always remain entangled, although their entanglement decays exponentially in the channel (see Chapters 2 and 3).

The preceding discussion highlights that entanglement (Section 1.5 and Chapter 3) is the *fundamental resource* for quantum communication, even when it is not directly used as a physical resource. Theoretical security proofs for unconditionally secure QKD, both for qubits [55] and for qumodes [56], are also most conveniently constructed with the help of entanglement distillation or quantum error correction (Chapter 5).

There are, of course, many quantum communication protocols where physical entangled states are used, the most prominent example of which is quantum teleportation (Section 1.6 and Chapter 4). In fact, quantum teleportation can be seen as the *fundamental protocol* for quantum communication. This becomes particularly clear when one attempts to extend quantum communication, including the QKD schemes described above, to large distances, where, for instance, a physical prepare-and-measure scheme over the entire channel distance would no longer be feasible. In this case, physical entangled states should be distributed over smaller channel segments and connected through teleportation. Eventually, quantum information can be teleported over the whole distance using the final, long-distance entangled pair (see Figure 1.10). Such an approach to long-distance quantum communication leads to the so-called quantum repeater which we shall discuss now.

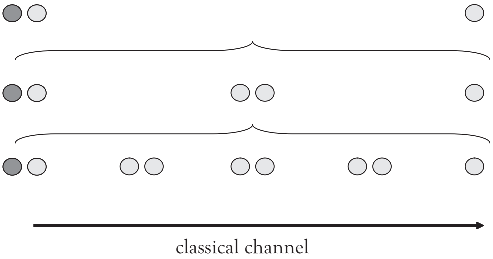

Figure 1.10 Transferring quantum information over large distances combining short-distance entanglement distribution, entanglement distillation, entanglement swapping, and quantum teleportation.

1.7.2 Repeaters and Relays

Light is an optimal information carrier for communication, and one may send quantum states encoded into a stream of single photons or a multi-photon pulse through an optical channel. However, quantum information encoded into fragile superposition states, for example, using photonic qubits or qumodes (Chapter 2), is very vulnerable against losses and other sources of excess noise along the channel such that the fidelity of the state transfer will exponentially decay with the length of the channel.

In long-distance, classical communication networks, signals that are gradually distorted during their propagation in a channel are repeatedly recreated through a chain of intermediate stations along the transmission line. For instance, optical pulses traveling through a glass fiber and being subject to photon loss can be reamplified at each repeater station. Such an amplification is impossible, when the signal carries quantum information. If a quantum bit is encoded into a single photon, its *unknown* quantum state cannot be copied along the line due to no-cloning; the photon must travel the entire distance with an exponentially decreasing probability to reach the end of the channel.

The solution to the problem of long-distance quantum communication is provided by the so-called quantum repeater [2, 3] (Figure 1.10). In this case, prior to the actual quantum-state communication, a supply of *known* quantum states, namely, standard entangled states, is generated and distributed among not too distant nodes of the channel. If a sufficient number of these imperfect entangled states are shared between the repeater stations, a combination of entanglement purification and swapping extends this shared entanglement over the entire channel. Through entanglement swapping [57] (Chapter 4), the entanglement of neighboring pairs is connected, gradually increasing the distance of the shared entanglement. The entanglement purification [22] (Chapter 5) enables one to distill (through local operations) a high-fidelity entangled pair from a larger number of low-fidelity entangled pairs, as they would emerge after a few rounds of entanglement swapping with imperfect entangled states and at the very beginning after the initial, imperfect entanglement generation and distribution between two neighboring repeater stations.

The essence of long-distance quantum communication as realized through the quantum repeater model [2, 3] can be summarized as follows: provided *sufficient local quantum memories* are available and *some form of quantum error detection* is applied, quantum communication over arbitrary distances is possible with an increase of (spatial or temporal) resources scaling only subexponentially with distance.

Note that the naive approach of dividing the total channel into several segments that are connected through quantum teleportation without incorporating any form of quantum error detection and without using quantum memories is not enough to render quantum communication efficient with regard to resource scaling. In this case, for instance, the probabilistic distribution of entangled pairs over the individual segments of the channel (Figure 1.10) must succeed at once. The number of pairs created over a total channel of length L per unit time interval (basically given by L_0/c with c, the speed of light in the channel and L_0, the length of each segment) is then proportional to

$$P_{\text{distr}}^{L/L_0} \times P_{\text{swap}}^{(L/L_0)-1} \,, \tag{1.114}$$

where P_{distr} is the success probability for obtaining an entangled pair in one segment, P_{swap} is the probability for a successful entanglement connection (swapping), L/L_0 is the number of segments, and so $(L/L_0)-1$ is the number of necessary swapping events. When either the distribution or the swapping is probabilistic,[27] $P_{\text{distr}} < 1$ or $P_{\text{swap}} < 1$, the pair creation rates will exponentially decay with the total distance L; even when, quite unrealistically, the initially generated pairs are perfectly entangled. Thus, in principle, if perfect local operations were available, the final pairs would have unit fidelities too with no need for any quantum error detection. This is the so-called *quantum relay*.[28]

Once perfect quantum memories are available, the exponential decay of the pair creation rate can be circumvented. For example, consider two neighboring segments. The time it takes in one segment to distribute a single pair is on average $(L_0/c)/P_{\text{distr}} \equiv T_0$. Now, a simultaneous distribution attempt in two segments will be successful in either one segment after approximately half that time period. The pair that is created first can then be stored in a quantum memory until the other segment has an entangled pair as well, after another waiting time of about T_0. Thus, after a time of roughly $3T_0/2$, two pairs will be present next to each other in the two neighboring segments [47] and one can proceed with the entanglement

[27] Which is usually unavoidable, see the discussions on the postselected generation and swapping schemes for polarization-encoded DV photonic qubits (Chapters 3 and 4). However, using CV qumode entangled states, entanglement generation and distribution (Chapter 3) as well as entanglement swapping (Chapter 4) are deterministic. In this case, the problem is an exponentially decaying fidelity requiring efficient quantum error detection techniques, which are hard to obtain in the CV setting (Chapter 5).

[28] Which, in the optical context (Chapter 2), may still help to enhance practicality of a scheme, for instance, in order to resolve single-photon signals against detector dark counts [47, 58–60].

swapping, with a total time of $(3T_0/2)/P_{\text{swap}} \equiv T_1$ to obtain one pair over double the elementary distance, $2L_0$.

In order to obtain two already swapped pairs (so each distributed over a distance of $2L_0$) next two each other, it will then take roughly a time of $3T_1/2$, and the corresponding next swapping step will lead to an entangled pair over distance $4L_0$ after a total average time of about $(3T_1/2)/P_{\text{swap}}$. Therefore, recursively, we end up having an average time of $(3/2)^n T_0/P_{\text{swap}}^n$, with $L/L_0 = 2^n$, for obtaining one pair over the total distance L. Compared with Eq. (1.114), this translates into a rate (number or pairs per time unit) proportional to

$$P_{\text{distr}} \left(\frac{2}{3} P_{\text{swap}}\right)^n = P_{\text{distr}} \left(\frac{2}{3} P_{\text{swap}}\right)^{\log_2(L/L_0)} \\ \propto (L/L_0)^{\log_2\left(\frac{2}{3} P_{\text{swap}}\right)} . \tag{1.115}$$

This is the *quantum repeater* in its simplest manifestation (using ideal memories and without purification), achieving a rate that scales only polynomially with the total distance L. The above approximation on the rates is good for small probabilities P_{distr} and P_{swap}. In the limit of unit P_{distr} and P_{swap}, of course, there is no need for memories and the relay performs as well as the repeater.

1.7.3 Shannon Theory

Prior to those proposals for the above-mentioned applications through which Alice and Bob take advantage of using quantum resources, earlier treatments of quantum communication aimed at deriving the fundamental limits imposed by quantum theory on the classical communication by means of quantum signals. A very famous result in this context is that from Holevo [61], sometimes referred to as the fundamental law of quantum communication [62]. It places an upper bound, the so-called *Holevo bound*, on the mutual information of Alice and Bob,

$$I(\text{A} : \text{B}) \le S(\hat{\rho}) - \sum_a p_a S(\hat{\rho}_a) \le S(\hat{\rho}) , \tag{1.116}$$

where $S(\hat{\rho})$ is the von Neumann entropy from Eq. (1.22), $\hat{\rho}$ is the mean channel state, and $\hat{\rho}_a$ are the signal states with a priori probabilities p_a. In this relation, equality is attained when Alice sends pure orthogonal signal states.[29)]

[29)] In classical information theory [63], the information content of a message depends on the probabilities p_a for the occurrence of a letter drawn from an alphabet A. The less frequent a letter occurs, the more information it carries. The average information content per letter is then $I(\text{A}) = -\sum_a p_a \log_2 p_a$ in units of bits. For two parties, a sender and a receiver corresponding to two alphabets A and B, the information in the communication channel is quantified by the so-called mutual information $I(\text{A} : \text{B}) = I(\text{A}) + I(\text{B}) - I(\text{A}, \text{B})$. Here, the sum $I(\text{A}) + I(\text{B})$ contains joint information in both alphabets, double counting the part which is mutual to both alphabets. By subtracting the actual expression for the joint information $I(\text{A}, \text{B}) = -\sum_{ab} p_{ab} \log_2 p_{ab}$, where the joint alphabet AB has letters with probabilities p_{ab}, the mutual information is obtained.

Even assuming an ideal (noiseless) channel, any attempt by Bob to retrieve the classical information sent from Alice introduces noise when the signal states are non-orthogonal. In fact, there is an optimal, *accessible information*, depending on the measurement strategy that Bob employs. The most general measurement strategy is described by a POVM $\{\hat{E}_b\}$ with $\sum_b \hat{E}_b = \mathbb{1}$. The accessible information is typically hard to compute.

When Bob is presented with a state $\hat{\rho}_a$ representing letter a from Alice's alphabet, he will instead find letter b from his own alphabet with a conditional probability given by $p_{b|a} = p_{ab}/p_a = \text{Tr}(\hat{E}_b \hat{\rho}_a)$. From this, one may usually compute the mutual information $I(\text{A} : \text{B}) = I(\text{A}) + I(\text{B}) - I(\text{A}, \text{B}) = \sum_{ab} p_{ab} \log_2(p_{ab}/(p_a p_b))$.

Now, the information-theoretic condition for secure communication, that is, for enabling extraction of a secure key using privacy amplification [64] and error correction techniques [65], is given by the following relation for the mutual information between the three participants, Alice, Bob, and Eve,

$$I(\text{A} : \text{B}) > \max\{I(\text{A} : \text{E}), I(\text{E} : \text{B})\} . \tag{1.117}$$

In other words, the mutual information between Alice and Bob, $I(\text{A} : \text{B})$, must exceed the information that either of them shares with Eve.[30)]

Finally, there is another entanglement-based quantum communication scheme which is kind of complementary to quantum teleportation. In this so-called *superdense coding* [67], the roles of the classical and quantum channels are interchanged relative to those in quantum teleportation. Instead of reliably transferring quantum information through a classical channel using entanglement as in quantum teleportation, in a superdense coding scheme, the amount of classical information transmitted from Alice to Bob is increased when Alice sends quantum information, namely, her half of an entangled state shared with Bob through a quantum channel to Bob.

For instance, two bits of classical information can be conveyed by sending just one qubit. Superdense coding relies upon the remarkable feature that, for instance, all four two-qubit Bell states in Eq. (1.93) can be transformed into each other through local Pauli operations. Thus, Alice, similar to what Bob does in quantum teleportation, applies one of four possible operations to her half of a shared Bell pair, thereby encoding two classical bits. Finally, Bob, similar to what Alice does in quantum teleportation, performs a Bell measurement on his half of the entangled pair together with Alice's half to retrieve the bit values. Therefore, Alice has to send her half through a quantum channel to Bob. In general, superdense coding aims at increasing the capacity (the maximal mutual information) of a communication channel using entanglement.

[30)] In a CV QKD scheme based upon coherent-state signals, initially, for losses in the channel greater than 3 dB, the condition $I(\text{A} : \text{B}) > I(\text{A} : \text{E})$ is always violated using the classical standard techniques. However, there are various methods to beat the 3 dB loss limit. One method is using, in addition to the classical techniques, entanglement distillation and quantum memories, which are both rather demanding in a realistic implementation (see Chapter 5). Alternative approaches include a "reverse reconciliation" protocol [52] with Alice guessing what was received by Bob instead of Bob guessing what was sent by Alice, and another method based upon postselection [66].

Like quantum teleportation, superdense coding relies on preshared entanglement. Thus, superdense coding is still in agreement with Holevo's rule that, at most, one classical bit can be transmitted by sending one qubit because, taking into account Bob's half of the entangled state transmitted to him prior to the actual communication ("offline"), in total, two qubits must be sent to Bob. This entanglement-based superdense coding must not be confused with other "quantum coding" schemes such as those introduced by Schumacher [68]. The Schumacher protocols enable Alice and Bob to approach the Holevo bound even for non-orthogonal or mixed signal states through appropriate encoding of the classical information into these states. This type of quantum coding, including the results of Holevo, may be considered as part of an extension of Shannon's classical information theory [69] to the quantum realm [4, 5].

Superdense coding, like quantum teleportation, can be similarly translated from qubits to qumodes in a CV superdense coding protocol [70, 71].[31]

Entanglement as a resource and quantum teleportation as a protocol are naturally associated with quantum communication, as we attempted to illustrate in this section. However, both are just as fundamental for quantum computation. This subject is discussed in the next section and in more detail in Chapters 6 and 7.

1.8 Quantum Computation

The ultimate real-world application of quantum theory would be the quantum computer. By processing quantum information encoded in a superposition of all possible classical inputs, a quantum computer is capable of simultaneously computing each output value for every possible input – a notion called quantum parallelism.

This field of quantum computation was initiated through Deutsch's work on universal quantum computation from 1985 [72], based on earlier ideas of Feynman [73]. Today, this field is divided into various subfields associated with complementary research efforts such as

- the search for quantum algorithms,
- proof-of-principle demonstrations of small-scale quantum circuits, and
- proofs of universality, fault-tolerance, and scalability.

Initially, quantum algorithms were only of interest to specialists in the field. However, when Shor discovered in 1994 how to factorize numbers into prime numbers significantly faster than classically (in polynomial rather than exponential time) by using a quantum algorithm [74], the possibility of realizing a quantum computer became a security issue. Codes such as the famous RSA encryption, considered ef-

[31] By utilizing the idealized, unphysical two-qumode entangled states of Eq. (1.95), similar to the qubit case, CV superdense coding would approach, in this idealized limit, a capacity twice as big as that theoretically attainable in the absence of entanglement [71].

fectively secure based upon a mathematically unproven complexity assumption,[32] became suddenly vulnerable; no longer due to the nonexistence of a mathematical proof, but rather because of a new type of computer whose existence is permitted by the laws of physics.

Ironically, the solution to the problem of unconditional security was also offered by quantum theory in form of quantum key distribution, as discussed in the preceding section. Even a quantum computer cannot render quantum cryptography insecure.

The probably most well-known quantum algorithms, besides Shor's, are Grover's algorithm of 1996 for searching a database [75] and the Deutsch–Jozsa algorithm of 1992 [76] which inspired the works of Shor and Grover. All these ideas have in common that they illustrate the potential of quantum information processing to provide solutions for problems that are defined in purely classical terms and (most likely) cannot be solved efficiently through classical information processing. Similar to what quantum cryptography achieves for classical communication, quantum algorithmic offers potentially better ways to perform certain classical computations; even though at intermediate stages, both the communications and computations would rely upon quantum resources and processing.

There are basically two main categories of quantum algorithms, namely, those based upon the quantum Fourier transform corresponding to general implementations of the so-called hidden subgroup problem and quantum search algorithms [5, 77]. The Shor and Deutsch–Josza algorithms belong to the former category, while the latter one consists of variations of the Grover algorithm. An example of a class of algorithms that fit in neither of these two categories is quantum simulation. In this case, the quantum computation is used to simulate a quantum system, as it was originally envisaged by Feynman [73]. The notion of simulating a Hamiltonian is the most convenient starting point for defining quantum computation over continuous quantum variables on qumodes. This will be discussed in Section 1.8.2.

Typically, however, a model of quantum computation or a specific algorithm will be implemented on qubits. In this case, an algorithm for N qubits, computed in a 2^N-dimensional Hilbert space, will convert initially unentangled qubit product states at some stages of the computation into a multi-party entangled state of many qubits. It was already mentioned in Section 1.1 that entanglement can be a *sufficient* resource for quantum computation, and the engineering and exploitation or consumption of (multi-party) entangled states for quantum information processing will be the central topic of the remainder of this book. However, we may as well ask: is entanglement also a *necessary* resource for quantum computation?

Indeed, the answer to this question is neither a clear yes nor a clear no. First of all, we may simply redefine the total physical system and replace the tensor-product Hilbert space of the N qubits, $\otimes^N \mathcal{H}_2$ (where $\mathcal{H}_k$ denotes a Hilbert space of dimension k), by an equivalent (isomorphic) Hilbert space for a single $d = 2^N$-level qudit system, $\mathcal{H}_{2^N}$. Eventually, we may argue that it is not some form

[32] That is, assuming that these codes are too hard to break by a classical computer. For instance, there is no classical algorithm known to factorize numbers in an efficient amount of time to break the RSA encryption.

of multi-party (multi-particle) entanglement, but rather the interference effect in complicated superposition states of a single qudit (particle) which is responsible for a quantum computational speed-up [78, 79]. However, should we always refer to a single-particle state such as

$$\frac{1}{\sqrt{2}}\left(|10\rangle + |01\rangle\right) \equiv \frac{1}{\sqrt{2}}\left(|\bar{0}\rangle + |\bar{1}\rangle\right) \tag{1.118}$$

as an unentangled state? More specifically, one physical manifestation of this kind of state would be a path-entangled state of two single-rail qubits, obtainable by splitting a single-photon wave-packet at a beam splitter (see Chapters 2 and 3; Figure 3.2), where $|10\rangle \equiv |1\rangle_1 \otimes |0\rangle_2$ represents a possible state of the two spatial modes one and two at the two output ports of the beam splitter. Alternatively, this state may as well be interpreted as a simple one-qubit $+X$-stabilizer state in polarization encoding (see Chapter 2), where this time, $|10\rangle \equiv |1\rangle_H \otimes |0\rangle_V \equiv |H\rangle \equiv |\bar{0}\rangle$ stands for a possible state of two orthogonal polarization modes; in this case, the horizontally polarized mode H is excited by a photon, while the vertically polarized mode V is in the vacuum state. In either case, the single-photon system lives in a (sub)space of two optical modes.

Regardless of whether the state in Eq. (1.118) is considered entangled or not,[33] extending the basis from two levels to 2^N levels would clearly provide enough (Hilbert) space to do quantum computation; either on a single 2^N-level system or on N two-level systems.[34] However, there is a crucial difference in terms of physical resources needed for realizing the quantum computations. For the N-qubit tensor-product-based quantum computer, N physical qubits (for instance, N polarization-encoded photons) will be needed, so that the physical resources scale linearly with the number of qubits. In contrast, a 2^N-level quantum computation in which, by definition, the multi-*party* entangled states are disguised as single-particle superposition states will always be at the expense of some exponential overhead in terms of physical resources (for instance, exponentially many optical elements for transforming 2^N optical modes or an exponentially increasing measurement precision). One may then argue that it is actually the multi-*particle* entanglement in

[33] For a nice discussion on this issue, see [80–82]. In [80], a simple argument explains why a single-particle two-mode state like that in Eq. (1.118) should be considered entangled, provided the two modes are spatially separated, which is the case for path-encoding, but not for polarization encoding. The two modes of the path-entangled state may then be distributed among two spatially separated two-level atoms and map the two atoms onto the clearly entangled two-particle state $\left(|eg\rangle + |ge\rangle\right)/\sqrt{2}$ through *local* atom-light interactions (here, the initial atomic ground states $|g\rangle$ would only become excited, $|e\rangle$, provided a photon is in the optical mode that interacts with the respective atom). Most importantly, in an optical state like that in Eq. (1.118), the two field modes are entangled and not the photon with the vacuum. Similarly, a low-squeezing two-mode squeezed state, $|00\rangle + r|11\rangle$ with $r \ll 1$, has a small amount of entanglement which is not between the two photons and the vacuum, but rather between the two qumodes (see Chapters 2 and 3). Multi-party entanglement between many qumodes will be introduced in Chapter 3.

[34] An example for the former type of quantum computation will be presented in Section 2.8 using 2^N optical modes for a single photon and linear optical elements.

the multi-qubit tensor-product approach that enables one to avoid the exponential overhead [78, 79].[35]

Compared to discrete qubit encodings, qumodes naturally offer any desirable amount of space to process quantum information. However, it is not obvious whether and how such analog quantum information can be exploited. Unphysical qumode stabilizer states such as the position eigenstates $|x\rangle$ are not available as a computational basis. Instead, Gaussian states such as squeezed states (see Chapter 2) would have to be employed. These physical states, though producible in highly efficient ways, can then only be measured at a finite resolution or in a probabilistic fashion. For example, in order to implement a CV version of the Deutsch–Josza algorithm, there would be an uncertainty-based trade-off between a position x-encoding and a p-measurement resolution; thus, preventing a computational speed-up [83]. In this case, the exponential overhead can be thought of as the requirement of an infinite measurement precision or the preparation of a quantum state with infinite energy. In many cases, it is not even clear how to recast a given computational problem and the corresponding quantum algorithm in the CV setting.

Besides quantum algorithmic, as listed at the beginning of this section, the two other main directions of current research on quantum computation are experimental demonstrations of small-scale quantum circuits, and theoretical proofs of universal (potentially scalable and fault-tolerant) models and approaches for quantum computation. The former topic will be addressed to a great extent in the remainder of this book. Universality, in the context of both qubit and qumode encodings and processing, shall be considered in the section after next. Now, we briefly introduce two equivalent, but conceptually very different models for quantum computation.

1.8.1
Models

There are various models to describe quantum computations of which the most common one is the *circuit* model [5]. It uses sequences of reversible, unitary gates in order to transform an input quantum state into any desired output quantum state. Although, finally, the output state must be measured for read-out, the largest part of the computation is conducted in a measurement-free fashion. The circuit model provides a natural language to describe quantum algorithms. Important notions such as universality can be conveniently expressed in the circuit model, as we will discuss in the next section.

A conceptually very different model for quantum computation is that of *measurement-based* quantum computing. As opposed to the standard circuit model, in measurement-based quantum computation, the quantum gates are embedded into an entangled state prior to the actual computation – the gates are performed "offline" on the entangled-state resource. This turns out to be of great importance

[35] However, there are specific examples of quantum algorithms which neither require multi-particle entanglement nor depend on an exponential overhead of spatial or temporal resources [79].

for experimental realizations because even highly probabilistic gate implementations can be useful, provided they are applied to the off-line state and a successfully transformed resource state is kept intact until its consumption during the online computation. In order to render measurement-based quantum computation (near-)deterministic despite the randomness induced by the measurements, typically, some form of measurement-dependent feedforward operations will be needed. Since an online, measurement-based computation is no longer reversible, such approaches to quantum computation are sometimes referred to as one-way models.

There are various specifications to measurement-based quantum computing. One approach is based upon a generalization of standard quantum teleportation [84]. In the qubit case, a single-qubit (multi-qubit) state is then teleported through a modified, unitarily transformed two-qubit Bell (multi-qubit entangled) state such that the desired gate operation is affected on the output state. This extension of the usual communication scenario for quantum teleportation with an ideally exact state transfer from Alice to Bob to gate teleportations for computation with a teleported state unitarily transformed depending on the modified resource state illustrates the general importance of quantum teleportation. Gate teleportation will be further discussed in Chapter 6.

In the standard version of gate teleportation, a *nonlocal* two-party Bell measurement projecting onto an entangled-state basis is still needed, which can be a severe complication for experimental implementations. However, there is an ultimate realization of measurement-based quantum computing in which all entangling operations are performed offline and for the actual computation, only *local* measurements are needed. In such a cluster-based one-way quantum computation [1], a multi-party entangled state is first prepared offline and the actual computation is then conducted solely through single-party projection measurements on the individual nodes of that resource state – the *cluster state*. By choosing appropriate measurement bases in each step, possibly depending on earlier measurement outcomes, any unitary gate can be applied to an input state which typically becomes part of the cluster at the beginning of the computation, see Figure 1.11.

The essence of cluster computation can be summarized as follows: the cluster state is *independent of the computation*; universality is achieved through *choice of*

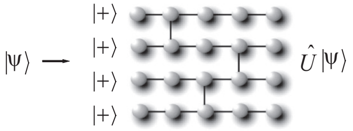

Figure 1.11 One-way cluster computation for qubits. Certain single-qubit stabilizer states become pairwise entangled to form a multi-qubit cluster state (see Section 3.1). Local projection measurements on the individual qubits, potentially including feedforward with a measurement order going from left to right, are then enough to realize (universal) quantum computation. A multi-qubit input state $|\psi\rangle$ attached to the left end of the cluster could, in principle, be (universally) processed with the output state occurring at the right end of the cluster. The vertical edges allow for two-qubit gates (more details can be found in Section 7.1).

measurement bases. A more detailed discussion of cluster computations on qubits and qumodes can be found in Chapter 7. Next, we turn to the notion of universality.

1.8.2 Universality

The two models of quantum computation as introduced in the preceding section, the circuit and the one-way model, are both known to be universal and in this sense, they can be considered equivalent models. So what does universality mean? Usually, universality is associated with the ability to apply an arbitrary unitary operator or matrix upon a given signal state, for instance, to an initial multi-qubit product state. Under certain circumstances, in particular, in realistic situations including experimental imperfections and errors, an exact implementation of a unitary matrix is not achievable and hence the notion of approximate, asymptotic universality becomes important. In this case, a universal set of elementary gates is considered that allows for approaching any given unitary gate at any desired precision through elementary-gate concatenations.

From a slightly different point of view, one may also think of universality as the ability to simulate any given Hamiltonian. This Hamiltonian approach to universality turns out to be particularly useful for qumode systems where the available transformations are naturally given in terms of interaction Hamiltonians which are polynomials of the bosonic mode operators. One possible way to understand this approach is to consider the following decomposition,[36]

$$e^{iH_2t}e^{iH_1t}e^{-iH_2t}e^{-iH_1t} = e^{[H_1,H_2]t^2} + O(t^3)\,. \tag{1.119}$$

Thus, by applying the Hamiltonians H_1 and H_2 for some short time, we can also approximately implement the Hamiltonian $-i[H_1, H_2]$, provided the interaction times are sufficiently short. Once the simplest commutator can be simulated, higher-order (nested) commutators are also available through further concatenation. Provided nested commutation of a set of elementary Hamiltonians allows one to generate an arbitrary Hamiltonian, the elementary set can be referred to as a universal set. This type of asymptotic, approximate model for universal quantum computation is applicable to both DV qubit [85] and CV qumode [86] systems on their own as well as to hybrid systems combining qubits and qumodes (see Chapter 8).

1.8.2.1 Qubits

Consider a single qubit and recall the discussion on single-qubit unitaries in Section 1.3.1. In the box at the end of Section 1.3.2, it is shown that an arbitrary single-qubit unitary can be expressed as $e^{i\phi}\hat{R}_s(\theta)$, depending on four real parameters

[36] Using $e^{A}e^{B} = e^{A+B}e^{[A,B]/2} + O([A,[A,B]],[[A,B],B])$ and so $e^{\pm iH_2t}e^{\pm iH_1t} = e^{\pm i(H_1+H_2)t}e^{-[H_2,H_1]t^2/2} + O(t^3)$, which is one of the well-known Baker–Campbell–Hausdorff (BCH) formulas, also commonly used in quantum optics (see Chapter 2). Here and in Eq. (1.119), we omitted the operator hats on the Hamiltonians.

determining ϕ, θ, and the real three-dimensional unit vector $\boldsymbol{s}$. Now, we can decompose this arbitrary rotation into a sequence of rotations around two fixed axes, for instance, the Z and Y axes,

$$e^{i\phi}\,\hat{R}_Z(\alpha)\,\hat{R}_Y(\beta)\,\hat{R}_Z(\gamma) = e^{i\phi}\,Z_\alpha\,Y_\beta\,Z_\gamma\ , \tag{1.120}$$

using the definitions given after Eq. (1.60), with real parameters ϕ, α, β, and γ. This can be easily seen by parameterizing an arbitrary, unitary 2×2 matrix with orthonormal rows and columns and decomposing it into a product of matrices [5].

From the preceding discussion, we learn that the set $\{Z_\theta, Y_{\theta'}\}$ represents a universal set for single-qubit unitaries; any single-qubit unitary can be constructed from a small sequence of Z and Y rotations. Moreover, the ability to perform these rotations precisely with angles α, β, and γ would mean that the set $\{Z_\theta, Y_{\theta'}\}$ allows for realizing any single-qubit unitary *exactly*. It can then be shown [5] that arbitrary unitaries in a multi-qubit space can be exactly realized through this universal set for single-qubit unitaries, together with one fixed two-qubit entangling gate such as the CNOT gate (see below). Hence, the set $\{Z_\theta, Y_{\theta'}\}$ supplemented by, for instance, the CNOT gate is universal for quantum computation in finite dimensions.

So why would we have to consider asymptotic, approximate realizations of unitaries or Hamiltonians as, for example, described by Eq. (1.119)? The problem with the set $\{Z_\theta, Y_{\theta'}\}$ is that it is continuous and so an arbitrary single-qubit rotation requires infinite precision for every rotation. This is hard to realize, especially in an error-resistant fashion. Therefore, it is useful to define a discrete, *finite* set of fixed elementary rotations which then can no longer achieve any multi-qubit unitary exactly as the whole set of unitary gates is continuous, but instead in an approximate fashion at arbitrary precision. In order to be efficient, a sufficiently good approximation must not require an exponential number of elementary gate applications.[37)]

A convenient universal set of gates is given by [5]

$$\{H, Z_{\pi/2}, Z_{\pi/4}, C_Z\}\ . \tag{1.121}$$

Here, H is the Hadamard gate, $H|k\rangle = (|0\rangle + (-1)^k|1\rangle)/\sqrt{2}$, needed in order to switch from gates diagonal in Z to gates diagonal in X. The two-qubit gate C_Z acts as an entangling gate, with

$$|k\rangle \otimes |l\rangle \to (-1)^{kl}|k\rangle \otimes |l\rangle\ , \quad k, l = 0, 1\ . \tag{1.122}$$

For convenience, we repeat the definition $Z_\theta \equiv e^{-i\theta Z/2}$ for a single-qubit rotation about the Z-axis by an angle θ with the computational Pauli operator Z acting as $Z|k\rangle = (-1)^k|k\rangle$; the conjugate Pauli operator X obtainable from Z through Hadamard describes bit flip operations, $X|k\rangle = |k \oplus 1\rangle$. Note that removing the

[37)] Indeed, there is the important issue here as to whether the number of elementary gate operations for simulating a given multi-qubit unitary scales subexponentially with the size of the exact circuit for any desired accuracy. Many multi-qubit unitaries cannot be efficiently simulated [5].

[38)] However, removing $Z_{\pi/2}$ from the elementary gate set would give the smaller set $\{H, Z_{\pi/4}, C_Z\}$ which is still universal, as we have $Z_{\pi/4}Z_{\pi/4} = Z_{\pi/2}$.

gate $Z_{\pi/4}$ from the elementary gate set means that only the Clifford unitaries (Section 1.3.1) can be realized, which are known to be insufficient for a quantum computational speed-up over classical computation.[38] For both universality and speed-up when computing with stabilizer states such as $|+\rangle^{\otimes N}$, the non-Clifford phase gate $Z_{\pi/4}$ must be included; otherwise, if only using the Clifford set $\{H, Z_{\pi/2}, C_Z\}$, the stabilizer states remain stabilizer states at all times since Pauli operators are only mapped back onto Pauli operators, see Eqs. (1.64) and (1.65). Obviously, this no longer allows for universality including universal state preparations. However, why does it also prevent a speed-up compared to classical computations?

We know that a single-qubit Pauli operator is Clifford-transformed into another Pauli operator. Hence, the evolution of the ith N-qubit stabilizer generator[39] corresponding to an N-party tensor product of Pauli operators, $g_i = X_{i1} \otimes X_{i2} \otimes \ldots X_{iN}$, is specified through $\sim N$ parameters. Here, X_{ik} can be any one of the single-qubit Pauli operators or the unity operator for the corresponding slot, including a sign choice $\pm$, with $k = 1, 2, \ldots, N$. Therefore, one can keep track of the evolution of the whole state by calculating the new stabilizer generators for every $i = 1, 2, \ldots, N$. As a result, $\sim N^2$ parameters have to be calculated at every step of the evolution, which can be done efficiently using a classical computer. The crucial element here is that during the entire Clifford evolution, every N-qubit stabilizer state is uniquely determined through N stabilizer generators $\langle g_1, g_2, \ldots, g_N\rangle$, even though the state's stabilizer group has 2^N elements.

In general, any quantum computation solely using Pauli and Clifford gates (which include the Hadamard and the C_Z gates) on stabilizer states, measurements in a Pauli basis, and classical feedforward can be efficiently simulated by a classical computer. This is the so-called *Gottesmann–Knill theorem*.

Before we turn our attention to universal sets for qumodes, we give a few additions to the preceding discussion. A more commonly used two-qubit entangling gate is the CNOT gate acting on two computational basis ($\pm Z$ stabilizer) states as

$$|k\rangle \otimes |l\rangle \to |k\rangle \otimes |l \oplus k\rangle \ , \tag{1.123}$$

where, here again, $\oplus$ denotes addition modulo 2. The CNOT gate can be obtained from the C_Z gate through local Hadamards,

$$(\mathbb{1} \otimes H) C_Z (\mathbb{1} \otimes H) = \text{CNOT} \ . \tag{1.124}$$

We have used the CNOT gate already in the circuit of qubit quantum teleportation of Figure 1.8, illustrating the usual convention for drawing this particular two-qubit entangling gate.

While the Clifford gate $Z_{\pi/2}$ maps stabilizer states back onto stabilizer states, for the non-Clifford gate $Z_{\pi/4}$, we obtain non-stabilizer states. In this case, for instance, instead of Eq. (1.64), we have now

$$\begin{aligned} Z_{\pi/4}|+\rangle &= \left(e^{-i\pi/8}|0\rangle + e^{+i\pi/8}|1\rangle\right)/\sqrt{2} \\ &= e^{-i\pi/8}\left(|0\rangle + e^{+i\pi/4}|1\rangle\right)/\sqrt{2} \ . \end{aligned} \tag{1.125}$$

[39] For a definition of stabilizers, see the discussion and the box in Section 1.9.

The resulting non-stabilizer state $(|0\rangle + e^{+i\pi/4}|1\rangle)/\sqrt{2}$ is sometimes referred to as the "magic state" [87]. Here, the Heisenberg evolution of the stabilizer X under the non-Clifford π/8-phase gate $Z_{\pi/4}$, $Z_{\pi/4}^{\dagger} X Z_{\pi/4} = 1/\sqrt{2}(X - Y)$, using Eq. (1.61), no longer gives a Pauli operator.

1.8.2.2 **Qumodes**

Consider now a single qumode and recall the discussion on single-qumode unitaries in Section 1.3.2. An arbitrary single-qumode unitary can be written as $\hat{U} = e^{-itH(\hat{a},\hat{a}^{\dagger})}$, with a general Hamiltonian $H(\hat{a}, \hat{a}^{\dagger})$ which is an arbitrary polynomial of the mode operators. Decomposing such a general Hamiltonian evolution into a set of elementary evolutions is a difficult task. In fact, for polynomials of arbitrary order in the mode operators, when the unitary on the qumode becomes a non-Clifford unitary, the Hamiltonian simulation will be, in general, only approximate and asymptotic, as expressed, for instance, by Eq. (1.119).

However, in the case of a single-qumode quadratic Hamiltonian corresponding to a Clifford unitary on the qumode, an *exact* decomposition similar to that in Eq. (1.120) is possible,[40] consisting of single-mode position-squeezers $\hat{S}(r)$ and phase rotations $\hat{R}(\theta)$ [recall the definitions in Section 1.3.2 and see Eq. (2.52) through Eq. (2.56)],

$$\hat{R}(\phi)\hat{S}(r)\hat{R}(\phi') \, . \tag{1.126}$$

More precisely, this decomposition only represents an arbitrary Clifford transformation up to displacements in phase space.[41] Therefore, the set $\{X(s), \hat{R}(\theta), \hat{S}(r)\}$, with the real parameters s, θ, and r, where we added the position-shift WH operator $X(s)$, is universal for arbitrary single-qumode Clifford unitaries (or, equivalently, Gaussian unitaries, see Chapter 2).

The three real parameters in Eq. (1.126) correspond to the three degrees of freedom needed for an arbitrary symplectic transformation on a single qumode. This decomposition can be obtained through Bloch–Messiah reduction [89] and generalized to an arbitrary number of qumodes (see Chapter 2). Note that the single-qumode Clifford set $\{X(s), \hat{R}(\theta), \hat{S}(r)\}$, though consisting of a finite number of elementary gates, is continuous, similar to the universal single-qubit set $\{Z_\theta, Y_{\theta'}\}$. Therefore, again, an *exact* realization of a single-qumode Clifford unitary would require infinite precision for implementing the parameters s, θ, and r, which correspond to effective interaction and free evolution times in the quantum optical

[40] Note that there are also exceptions of cubic or higher-order Hamiltonians which are exactly decomposable into lower-order Hamiltonians. For instance, $e^{-i\kappa\hat{x}^3} e^{it\hat{p}^2} e^{i\kappa\hat{x}^3} = e^{it(\hat{p}+3\kappa\hat{x}^2/2)^2}$, where the right-hand side has a fourth-order Hamiltonian, while the left-hand side only has second and cubic orders [88].

[41] The qumode Clifford group is a group whose generators are polynomials up to quadratic order in position $\hat{x}$ and momentum $\hat{p}$. Its group elements correspond to the unitary Gaussian transformations (see Chapter 2). For the general case of N qumodes, the Clifford group Cl(N) is a semidirect product of the symplectic group and the WH group, $\mathrm{Cl}(N) = \mathrm{Sp}(2N, \mathbb{R}) \ltimes \mathrm{WH}(N)$. According to our definition of the Clifford group in Eq. (1.69), the group WH(N) is a homogeneous space under the adjoint action of Cl(N), and one can construct a group representation of Cl(N) on the vector space of the Lie algebra wh(N).

context. Rather than attempting to get rid of this type of infiniteness, the purpose of constructing a *universal* single-qumode set (including non-Clifford unitaries) is primarily to simulate Hamiltonians of *arbitrary* order while still using a *finite* set of gates. As opposed to an exact Clifford simulation expressed by the symplectic transformation in Eq. (1.126) plus an additional complex phase-space displacement,[42] where each elementary gate may have arbitrary strength, the universal simulation is no longer possible without asymptotic concatenations like those in Eq. (1.119), requiring near-unity gates for each individual step.

Once arbitrary single-qumode Hamiltonians are available (in the asymptotic sense), it can be shown that, similar to the qubit case, arbitrary multi-qumode unitaries can be realized through the corresponding universal set for single-qumode unitaries, together with one fixed two-qumode Clifford gate [86, 90]. A two-qumode gate serving this purpose is the Clifford C_Z gate used below. Since the C_Z gate itself can be decomposed into a circuit of two two-qumode beam splitters and two single-qumode squeezers [89], the only entangling interactions needed for universal multi-qumode processing are provided by passive beam splitting transformations (see Chapter 2 for more details).

As a finite, elementary gate set for asymptotic simulations of arbitrary multi-qumode Hamiltonians, one may choose [90]

$$\{F, Z(s), D_2(t), D_3(\kappa), C_Z\}\ , \tag{1.127}$$

with $s, t, \kappa \in \mathbb{R}$. Now, F represents the Fourier transform operator that maps between the position and momentum basis states, $F|x\rangle_x = |x\rangle_p$. It is needed in order to switch from gates diagonal in $\hat{x}$ to gates diagonal in $\hat{p}$ since all the remaining gates are chosen to be diagonal in $\hat{x}$. The entangling gate C_Z is an x-controlled p-displacement, $C_Z = \exp(2\mathrm{i}\hat{x}_1 \otimes \hat{x}_2) = Z_1(\hat{x}_2) = Z_2(\hat{x}_1)$, with

$$C_Z|x\rangle_x|p\rangle_p = |x\rangle_x|p + x\rangle_p\ , \tag{1.128}$$

or, $C_Z^\dagger \hat{x}_{1,2} C_Z = \hat{x}_{1,2}$, $C_Z^\dagger \hat{p}_{1,2} C_Z = \hat{p}_{1,2} + \hat{x}_{2,1}$. The other $\hat{x}$-diagonal gates are the WH momentum shift operator, $Z(s) = \exp(2\mathrm{i}s\hat{x})$ with $Z(s)|p\rangle_p = |p + s\rangle_p$, and the phase gates $D_k(t) = \exp(\mathrm{i}t\hat{x}^k)$. The quadratic phase gate ($k = 2$) incorporates single-qumode squeezing (together with a rotation) and is sufficient in order to exactly simulate any multi-qumode Clifford (Gaussian) transformation (together with F, $Z(s)$, and C_Z). In order to asymptotically achieve universal multi-qumode processing including non-Clifford (non-Gaussian) unitaries, the additional cubic phase gate ($k = 3$) is needed.[43] in an efficient way.

[42] Obtainable from $X(s)$ through Fourier rotations $\hat{R}(-\pi/2)$.

[43] Similar to the qubit case, while removing the non-Clifford phase gate $D_3(t)$ renders the remaining Clifford set non-universal, removing the Clifford phase gate $D_2(t)$ gives a smaller, but still universal set. For example, in Eq. (1.131), the right-hand side contains a quadratic squeezing gate; thus, we can still obtain arbitrary Clifford gates [88]. From a practical point of view, however, it is better to implement Clifford unitaries whenever needed through Clifford gates (see Chapter 2).

Similar to the qubit stabilizer evolution under the qubit Clifford phase gate in Eq. (1.65), here, we obtain the qumode stabilizer evolution,[44]

$$\begin{aligned} X(s) \to D_2(t)X(s)D_2^\dagger(t) &= \mathrm{e}^{\mathrm{i}t\hat{x}^2} X(s)\mathrm{e}^{-\mathrm{i}t\hat{x}^2} \\ &= \mathrm{e}^{\mathrm{i}ts^2} X(s)Z(ts) \, . \end{aligned} \tag{1.129}$$

The conjugate stabilizer is invariant, $Z(s) \to D_2(t)Z(s)D_2^\dagger(t) = Z(s)$. These equations correspond to the following *linear* Heisenberg evolution equations for the position and momentum of a single qumode,

$$\begin{aligned} \hat{x} &\to D_2^\dagger(t)\hat{x}D_2(t) = \hat{x} \, , \\ \hat{p} &\to D_2^\dagger(t)\hat{p}D_2(t) = \hat{p} + t\hat{x} \, . \end{aligned} \tag{1.130}$$

In contrast, the non-Clifford, cubic phase gate transforms the X stabilizer as[45]

$$\begin{aligned} X(s) \to D_3(t)X(s)D_3^\dagger(t) &= \mathrm{e}^{\mathrm{i}t\hat{x}^3} X(s)\mathrm{e}^{-\mathrm{i}t\hat{x}^3} \\ &= X(s)Z(3ts^2/2)\mathrm{e}^{3\mathrm{i}st\hat{x}^2} \\ &= X(s)Z(3ts^2/2)D_2(3ts) \, . \end{aligned} \tag{1.131}$$

Instead of a multiple of WH operators, a product of quadratic and linear gates is obtained. The stabilizer $Z(s)$ remains unchanged. This is similar to what we found for qubits after performing the $\pi/8$-phase gate $Z_{\pi/4}$ on the Pauli X operator, which no longer gave a Pauli product. On the level of the WH generators, that is, in the Heisenberg evolution of the position and momentum operators, the momentum is no longer mapped onto a linear combination of the generators,

$$\begin{aligned} \hat{x} &\to D_3^\dagger(t)\hat{x}D_3(t) = \hat{x} \, , \\ \hat{p} &\to D_3^\dagger(t)\hat{p}D_3(t) = \hat{p} + \frac{3}{2}t\hat{x}^2 \, . \end{aligned} \tag{1.132}$$

The momentum transformation becomes *nonlinear*.[46]

The Gottesmann–Knill theorem that we had introduced in the preceding section for qubits applies to qumodes too [90]. In this case, the Clifford evolution of the stabilizers is most conveniently expressed in terms of the linear evolution of the WH generators $\hat{x}$ and $\hat{p}$. Similar to the discussion for qubits, the ith N-qumode stabilizer generator is determined through $\sim N$ parameters. For instance, the N positions of an initial product state of N position eigenstates are each transformed into position-momentum linear combinations with $2N$ real coefficients. Hence, the to-

[44] Which corresponds to the inverse Heisenberg evolution, while the actual Heisenberg evolution is $D_2^\dagger(t)X(s)D_2(t) = D_2^\dagger(t)\mathrm{e}^{-2\mathrm{i}s\hat{p}}D_2(t) = \mathrm{e}^{-2\mathrm{i}s(\hat{p}+t\hat{x})} = \mathrm{e}^{-\mathrm{i}ts^2}X(s)Z(-ts)$ using Eq. (1.130) and one of the BCH formulas.

[45] While the actual Heisenberg evolution is $D_3^\dagger(t)X(s)D_3(t) = \mathrm{e}^{-\mathrm{i}t\hat{x}^3}\mathrm{e}^{-2\mathrm{i}s\hat{p}}\mathrm{e}^{\mathrm{i}t\hat{x}^3} = \mathrm{e}^{-2\mathrm{i}s(\hat{p}+3t\hat{x}^2/2)} = X(s)Z(-3ts^2/2)\mathrm{e}^{-3\mathrm{i}ts\hat{x}^2}$ using one of the BCH formulas.

[46] In these Heisenberg equations, we use our usual convention of $\hbar = 1/2$. In general, using the commutator $[\hat{x}, \hat{p}] = \mathrm{i}\hbar$, and so $[\hat{x}^2, \hat{p}] = 2\mathrm{i}\hbar\hat{x}$ and $[\hat{x}^3, \hat{p}] = 3\mathrm{i}\hbar\hat{x}^2$, we obtain $D_2^\dagger(t)\hat{p}D_2(t) = \hat{p}+[\hat{p}, \mathrm{i}t\hat{x}^2] = \hat{p}+2\hbar t\hat{x}$ and $D_3^\dagger(t)\hat{p}D_3(t) = \hat{p} + [\hat{p}, \mathrm{i}t\hat{x}^3] = \hat{p} + 3\hbar t\hat{x}^2$, using the BCH formula $\mathrm{e}^{-\mathrm{B}}\mathrm{A}\mathrm{e}^{\mathrm{B}} = \mathrm{A} + [\mathrm{A}, \mathrm{B}] + 1/2![[\mathrm{A}, \mathrm{B}], \mathrm{B}] + 1/3![[[\mathrm{A}, \mathrm{B}], \mathrm{B}], \mathrm{B}] + \ldots$

tal evolution is completely specified through $2N^2$ real parameters. For the more interesting case of physical stabilizer states corresponding to Gaussian states (see Chapters 2 and 3), instead of the $2N^2$ real coefficients, $2N^2$ complex coefficients are needed, corresponding to $4N^2$ real parameters. The formalism of complex-valued stabilizers for physical qumode stabilizer states and their Clifford evolution will be discussed in Chapters 2 and 3. The Gottesmann–Knill theorem for qumodes then states that Gaussian operations on Gaussian states can be efficiently simulated classically [90].

Similar to the qubit case, one may also consider a CNOT gate for qumodes. This is defined as CNOT $= \exp(-2\mathrm{i}\hat{x}_1 \otimes \hat{p}_2) = X_2(\hat{x}_1) = Z_1(-\hat{p}_2)$, corresponding to an x-controlled x-displacement of mode 2 and a p-controlled p-displacement of mode 1: $\hat{x}_2 \rightarrow \hat{x}_1 + \hat{x}_2$, $\hat{p}_1 \rightarrow \hat{p}_1 - \hat{p}_2$, $\hat{x}_1 \rightarrow \hat{x}_1$, and $\hat{p}_2 \rightarrow \hat{p}_2$. As opposed to the C_Z gate, CNOT is no longer symmetric under exchange of the two modes. The CNOT gate can be obtained from the C_Z gate through local Fourier transforms,

$$(\mathbb{1} \otimes F^\dagger) \exp(2\mathrm{i}\hat{x}_1 \otimes \hat{x}_2)(\mathbb{1} \otimes F) = \exp(-2\mathrm{i}\hat{x}_1 \otimes \hat{p}_2) \ . \tag{1.133}$$

Universal sets

⊙ **Qubits**

$$\{H, Z_{\pi/2}, Z_{\pi/4}, C_Z\}$$

single-qubit gates: Z-Pauli (phase flip):

$$Z|\pm\rangle = |\mp\rangle \ , \quad Z|k\rangle = (-1)^k|k\rangle$$

general Z-rotation:

$$Z_\theta = \exp(-\mathrm{i}\theta Z/2)$$

$\pi/4$-phase gate:

$$Z^\dagger_{\pi/2} Z Z_{\pi/2} = Z \ , \quad Z^\dagger_{\pi/2} X Z_{\pi/2} = -Y \quad \text{(Clifford)}$$

$\pi/8$-phase gate:

$$Z^\dagger_{\pi/4} Z Z_{\pi/4} = Z \ , \quad Z^\dagger_{\pi/4} X Z_{\pi/4} = \frac{1}{\sqrt{2}}(X - Y) \quad \text{(non-Clifford)}$$

Hadamard:

$$H|k\rangle = \frac{|0\rangle + (-1)^k|1\rangle}{\sqrt{2}} \ , \quad HXH = Z \ , \quad HZH = X \quad \text{(Clifford)}$$

X-Pauli (bit flip):

$$X|k\rangle = |k \oplus 1\rangle \ , \quad X|\pm\rangle = \pm|\pm\rangle$$

two-qubit gate:

$$C_Z|k\rangle \otimes |l\rangle = (-1)^{kl}|k\rangle \otimes |l\rangle \quad \text{(Clifford)}$$

∿∿∿∿ **Qumodes**

$$\{F, Z(s), D_2(t), D_3(\kappa), C_Z\}$$

single-mode gates: WH-momentum shift:

$$Z(s)|p\rangle = |p + s\rangle\ , \quad Z(s)|x\rangle = \mathrm{e}^{2\mathrm{i}sx}|x\rangle$$

general phase (momentum) gate:

$$D = \exp[\mathrm{i}\, f(\hat{x})]\ , \quad \text{for example} \quad D_k(t) = \exp(\mathrm{i}t\hat{x}^k)$$

quadratic gate:

$$D_2^\dagger(t)\hat{x}\,D_2(t) = \hat{x}\ , \quad D_2^\dagger(t)\hat{p}\,D_2(t) = \hat{p} + t\hat{x} \quad \text{(Clifford)}$$

cubic gate:

$$D_3^\dagger(t)\hat{x}\,D_3(t) = \hat{x}\ , \quad D_3^\dagger(t)\hat{p}\,D_3(t) = \hat{p} + \frac{3}{2}t\hat{x}^2 \quad \text{(non-Clifford)}$$

Fourier:

$$F|x\rangle_{\text{pos}} = \int \mathrm{d}y\mathrm{e}^{2\mathrm{i}xy}|y\rangle_{\text{pos}} = |x\rangle_{\text{mom}}\ ,$$
$$F^\dagger\hat{p}\,F = \hat{x}\ , \quad F^\dagger\hat{x}\,F = -\hat{p} \quad \text{(Clifford)}$$

WH-position shift:

$$X(s)|x\rangle = |x + s\rangle\ , \quad X(s)|p\rangle = \mathrm{e}^{-2\mathrm{i}sp}|p\rangle$$

two-mode gate:

$$C_Z = \exp(2\mathrm{i}\hat{x} \otimes \hat{x}) : C_Z|x\rangle_{\text{pos}}|p\rangle_{\text{mom}} = |x\rangle_{\text{pos}}|p + x\rangle_{\text{mom}}\ ,$$
$$C_Z^\dagger\hat{x}_{1,2}C_Z = \hat{x}_{1,2}\ , \quad C_Z^\dagger\hat{p}_{1,2}C_Z = \hat{p}_{1,2} + \hat{x}_{2,1} \quad \text{(Clifford)}$$

Again, similar to the qubit case, the "magic state" for qumodes is obtained by applying the non-Clifford, cubic phase gate upon a zero-momentum eigenstate,

$$D_3(t)|p = 0\rangle = \mathrm{e}^{\mathrm{i}t\hat{x}^3}\frac{1}{\sqrt{\pi}}\int \mathrm{d}x|x\rangle = \frac{1}{\sqrt{\pi}}\int \mathrm{d}x\mathrm{e}^{\mathrm{i}tx^3}|x\rangle\ . \tag{1.134}$$

This is the so-called cubic phase state [28].

In the current section, we attempted to give an overview of various important notions in quantum computation including those of universality and scalability in the context of both qubit and qumode approaches. Universality in either approach will require some form of nonlinearity which may only be indirectly incorporated into a quantum computation through measurements or directly through some effectively enhanced weak nonlinear interaction. In the former scenario, a measurement-based model of quantum computation is applied, as we shall discuss in the context of experimental implementations in Chapters 6 and 7. The idea of weak nonlinear interactions is most intuitively realized in hybrid protocols in which both qubit and qumode systems participate (see Chapter 8). Once universality is achieved, including non-Clifford gates, in principle, a quantum computation can no longer be simulated classically in an efficient way.

Even when universality can be attained in principle, scalability remains a subtle issue. This issue will be part of the subsequent discussions on optical approaches to quantum computation.

Another topic of great importance is fault tolerance. Without some form of (concatenated) quantum error correction, a quantum computer will remain a theoretical construct. As we discussed before, quantum communication too must rely upon some form of quantum error detection when it is to be extended over larger distances. A complete treatment of fault tolerance for quantum information processing and computation is beyond the scope of this introductory chapter on quantum information. Nonetheless, in the next section, we shall at least mention the basic concepts of quantum error correction.

1.9
Quantum Error Correction

Quantum information processing and computation became an area of practical interest with potential real-world applications only after the discovery of quantum error correction (QEC) codes [5, 21, 91, 92]. Shor's code [21] was proposed at a time when people believed that QEC unlike classical error correction would be impossible. These initial doubts originated mainly from two supposed obstacles.

First, in classical error correction, the most natural way for protecting information against errors is to use *redundancy*. However, to create redundancy in the quantum case (by encoding qubits into multiple copies of the same qubits) appeared to be forbidden even in principle by the quantum mechanical no-cloning theorem (recall Section 1.1). Further, a second complication seemed to exist, following from the fundamental nature of quantum information: encoded into complex-amplitude superposition states, as opposed to classical digital information, quantum information is inherently *continuous*. This even holds for just a single qubit.

Despite these initial doubts, Shor's discovery and the many subsequent results on QEC demonstrated that there are two specific solutions to the two main problems mentioned in the preceding paragraph. A kind of redundancy can be obtained in the quantum case by encoding quantum information globally into *entangled*

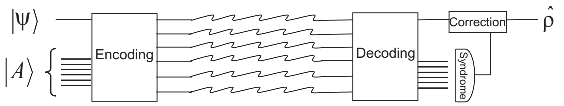

Figure 1.12 Basic elements of quantum error correction. Most commonly, the signal state $|\psi\rangle$ and a set of ancillae in some standard initial state $|A\rangle$ are unitarily transformed into an encoded state. After the effect of the errors, typically assumed to occur individually and independently on every subsystem, a unitary decoding circuit and a subsequent syndrome measurement of the ancillae reveal the type and location (and, for example, for qumodes, also the size) of the error. A final correction operation on the signal system will then recover the original state with a fidelity greater than that for an unprotected signal state, depending on the correctable set of errors for the specific code and on the actual error model.

states that are defined in a larger Hilbert space than the original signal space. These encoded states do not correspond to multiple copies of the original state and so do not violate no-cloning. For example, an arbitrary qubit state, $|\psi\rangle = a|0\rangle + b|1\rangle$, may be encoded into an entangled state of three physical qubits as[47]

$$|\psi\rangle \otimes |0\rangle \otimes |0\rangle \rightarrow a|000\rangle + b|111\rangle \neq |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle . \qquad (1.135)$$

This encoding can be achieved by pairwise applying two CNOT gates upon the signal qubit together with the first ancilla qubit as well as with the second one. Eventually, local bit-flip errors occurring on exactly one of the three qubits can be detected and corrected, as we shall discuss in more detail shortly. The detection of the error will depend on some form of measurement, and it is this so-called syndrome measurement step which enables one to correct arbitrary, even continuous errors. This effect is called *discretization* of errors because a continuous error is reduced to a finite, discrete set of Pauli errors. We will illuminate this essential feature of QEC in the following section. Figure 1.12 shows the basic elements of QEC as applicable to both qubits and qumodes.

1.9.1 Discretization

In the preceding section, we wrote universal sets for qubits and qumodes in terms of single-variable gates, that is, gates diagonal in the computational variables Pauli Z and position $\hat{x}$, respectively. For universality, at least one diagonal gate needed to have a rotation angle $\neq k\pi/2$ on the Bloch sphere for qubits and a Hamiltonian of $>$ quadratic order for qumodes. In addition, the Hadamard and the Fourier gates were required in order to affect multi-variable gates.

The simplest manifestation of a QEC code also works with single-variable gates. However, quite remarkably, universality, that is, universal protection against *arbitrary* single-variable errors (including non-Clifford-type errors) follows directly

[47] Recall the discussion of the preceding section. The state in Eq. (1.135) may as well be interpreted as a certain superposition state of an eight-level particle. However, in this case, encoding, occurrence of local errors, and syndrome identification lack the nice physical and operational meaning of the multi-particle scenario.

from the ability of a code to correct the simplest single-variable errors, for instance, Pauli X bit-flip errors for qubits and WH $X(s)$ position shift errors for qumodes. Let us see how this works.

Consider a single qubit in an arbitrary state, $|\psi\rangle = a|0\rangle + b|1\rangle$. First, the error model shall be described by a simple one-qubit bit flip Pauli channel, with $\mathcal{E}(\hat{\rho}) = (1-p)\hat{\rho} + pX\hat{\rho}X$ (see Section 1.4.1): with probability p a bit flip occurs; otherwise, the state remains unchanged. So the error set is discrete and finite, consisting only of Pauli X errors. Hence, the correctable error set should contain at least one-qubit X errors. Using the encoded state in Eq. (1.135) and applying the channel map upon every physical qubit independently gives the output density operator,

$$\begin{aligned}(1-p)^3\hat{\rho}_{\text{enc}} &+ p(1-p)^2\sum_{k=1}^{3} X_k\hat{\rho}_{\text{enc}}X_k \\ &+ p^2(1-p)\sum_{l<k=2}^{3}(X_l\otimes X_k)\hat{\rho}_{\text{enc}}(X_l\otimes X_k) + p^3X^{\otimes 3}\hat{\rho}_{\text{enc}}X^{\otimes 3}\,, \qquad (1.136)\end{aligned}$$

with $\hat{\rho}_{\text{enc}} \equiv (a|000\rangle + b|111\rangle)(a^*\langle 000| + b^*\langle 111|)$. Now, if we were able to discriminate the orthogonal subspaces spanned by $\{|000\rangle, |111\rangle\}$ and $\{X_k|000\rangle, X_k|111\rangle\}$ with $k = 1, 2, 3$, without changing the original amplitudes of the corresponding terms, we could at least identify the errors up to $O(p^2)$. In fact, the three-qubit code achieves exactly this. It uses four orthogonal subspaces, each two-dimensional with enough space to preserve the original qubit, which correspond to the four cases of no error at all and a bit-flip error occurring on any one of the three qubits. As a result, through the three-qubit repetition code, the effective error probability is reduced from p to p^2. Higher repetitions may lead to even better error suppression.

From this, it also becomes clear why two physical qubits are not enough for such a bit-flip code: in the four-dimensional physical Hilbert space of two qubits, there are only two possible orthogonal, two-dimensional subspaces; not enough for obtaining and discriminating all the three cases of an error occurring on either qubit ($\{X_k|00\rangle, X_k|11\rangle\}$), with $k = 1, 2$, and no error happening at all ($\{|00\rangle, |11\rangle\}$), which would require six physical dimensions. However, if we are satisfied with only detecting whether an error occurred (without correcting it), two qubits would be enough since the no-error subspace $\{|00\rangle, |11\rangle\}$ can still be discriminated from the error subspaces $\{X_k|00\rangle, X_k|11\rangle\}$. In general, this dimensional argument tells us how many physical qubits will be needed for a given error model and a desired correctable error set.

Now, let us consider a channel which is more general than the bit-flip channel and allow for an arbitrary X-error, that is, an arbitrary X-rotation $X_\theta = e^{-i\theta X/2} = \cos(\theta/2)\mathbb{1} - i\sin(\theta/2)X$. In this case, using again the three-qubit code, we would still be able to correct the dominating errors by discriminating the orthogonal subspaces $\{|000\rangle, |111\rangle\}$ and $\{X_k|000\rangle, X_k|111\rangle\}$ with $k = 1, 2, 3$. In fact, the syndrome measurements that achieve this discrimination will reduce the total density operator again to terms which have no error at all or a bit flip on exactly one qubit in the leading order. More precisely, only terms like $p(1-p)^2\cos^2(\theta/2)\hat{\rho}_{\text{enc}}$ and $p(1-$

$p)^2 \sin^2(\theta/2) X_k \hat{\rho}_{\mathrm{enc}} X_k$ with $k = 1, 2, 3$ will remain after the syndrome detection, and the off-diagonal terms like, for instance, $p(1-p)^2 \mathrm{i} \cos(\theta/2) \sin(\theta/2) \mathbb{1} \hat{\rho}_{\mathrm{enc}} X_k$ vanish. In other words, even though the original error is a continuous X-rotation, due to the syndrome measurement, this error *will become* a simple Pauli X error or result in no error at all. The final correction operation then works as before by just unflipping the corrupted qubit.

Now, consider a single qumode in an arbitrary state, $|\psi\rangle = \int \mathrm{d}x \, \psi(x)|x\rangle$. A (perfectly) repetition-encoded three-qumode state in this case becomes

$$\int \mathrm{d}x \, \psi(x)|x\rangle \otimes |x\rangle \otimes |x\rangle \, . \tag{1.137}$$

Now, whenever exactly one qumode is subject to an arbitrary $\hat{x}$-error, acting as $\mathrm{e}^{\mathrm{i}f(\hat{p})}$, the syndrome detection discriminating between the subspaces $\{X_k(s)|xxx\rangle | \, \forall x \in \mathbb{R}\}$ with $k = 1, 2, 3$ and $s \in \mathbb{R}$ would result in a state where exactly one qumode is corrupted by a simple position shift. Since the location and the size of this position shift will be known from the syndrome measurement, the original, uncorrupted state can be recovered through a simple displacement operation on the corresponding qumode. For example, $\mathrm{e}^{\mathrm{i}f(\hat{p})}$ acting upon qumode 1 leads to

$$\begin{aligned}
\mathrm{e}^{\mathrm{i}f(\hat{p}_1)} \int \mathrm{d}x \, \psi(x)|xxx\rangle &= \mathrm{e}^{\mathrm{i}f(\hat{p}_1)} \int \mathrm{d}x \, \psi(x) \frac{1}{\sqrt{\pi}} \int \mathrm{d}p \, \mathrm{e}^{-2\mathrm{i}xp} |pxx\rangle \\
&= \frac{1}{\sqrt{\pi}} \int \mathrm{d}x \mathrm{d}p \, \psi(x) \mathrm{e}^{-2\mathrm{i}xp} \mathrm{e}^{\mathrm{i}f(p)} |pxx\rangle \\
&= \frac{1}{\pi} \int \mathrm{d}x \mathrm{d}y \mathrm{d}p \, \psi(x) \mathrm{e}^{2\mathrm{i}(y-x)p} \mathrm{e}^{\mathrm{i}f(p)} |yxx\rangle \, .
\end{aligned} \tag{1.138}$$

The syndrome identification amounts to projecting qumodes 1 and 2 as well as qumodes 2 and 3 onto the two-qumode projectors $\int \mathrm{d}z |z, z - u_k\rangle\langle z, z - u_k|$ with syndromes u_1 and u_2. In terms of the position operators, this corresponds to measurements of the relative positions $\hat{x}_1 - \hat{x}_2$ and $\hat{x}_2 - \hat{x}_3$ with outcomes u_1 and u_2, respectively. When the error $\mathrm{e}^{\mathrm{i}f(\hat{p})}$ occurred on qumode 1, we will always obtain $u_2 = 0$, whereas the other projector gives

$$\begin{aligned}
&\int \mathrm{d}z |z, z - u_1\rangle\langle z, z - u_1| \frac{1}{\pi} \int \mathrm{d}x \mathrm{d}y \mathrm{d}p \, \psi(x) \mathrm{e}^{2\mathrm{i}(y-x)p} \mathrm{e}^{\mathrm{i}f(p)} |yxx\rangle \\
&= \frac{1}{\pi} \int \mathrm{d}x \mathrm{d}y \mathrm{d}p \, \psi(x) \mathrm{e}^{2\mathrm{i}(y-x)p} \mathrm{e}^{\mathrm{i}f(p)} \delta(y - u_1 - x) |y, y - u_1, x\rangle \\
&= \frac{1}{\pi} \int \mathrm{d}x \mathrm{d}p \, \psi(x) \mathrm{e}^{2\mathrm{i}u_1 p} \mathrm{e}^{\mathrm{i}f(p)} |x + u_1, x, x\rangle \\
&= \mathrm{g}(u_1) \int \mathrm{d}x \, \psi(x) |x + u_1, x, x\rangle \, .
\end{aligned} \tag{1.139}$$

Though the function $g(u_1) \equiv (1/\pi \int \mathrm{d}p \mathrm{e}^{2\mathrm{i}u_1 p} \mathrm{e}^{\mathrm{i}f(p)})$ is a measurement-dependent prefactor, the conditional state for every syndrome u_1 becomes $\int \mathrm{d}x \, \psi(x)|x + u_1, x, x\rangle$ which can be corrected as described above. Note that for simplicity, we have used unnormalized states here and syndrome detections with infinite resolution. In the realistic case, the encoded state would correspond to a three-mode Gaussian state[48] producible with two squeezed-state ancillary qumodes using beam splitters (see Chapters 2 and 5). The infinitely precise measurement should be more realistically described by a finite syndrome window with projectors $\int_\Delta \mathrm{d}u_k \int \mathrm{d}z |z, z - u_k\rangle\langle z, z - u_k|$. So when, for instance, $g(u_1) = \delta(u_1)$ for the no-error case with $\mathrm{e}^{\mathrm{i} f(p)} \equiv 1$, we would obtain $\int_{-\Delta/2}^{\Delta/2} \mathrm{d}u_1 g(u_1) \int \mathrm{d}x \psi(x)|x + u_1, x, x\rangle = \int \mathrm{d}x \psi(x)|x, x, x\rangle$ as the final state.

To summarize, the mechanism for correcting arbitrary single-variable errors is very similar for qubits and for qumodes. In either case, even when an arbitrary error diagonal in, for example, X (qubits) and $\hat{p}$ (qumodes) may disturb a quantum state in infinitely many ways, the syndrome detection will map the original error onto a simpler error from a smaller error set: for qubits, this would be a flip in the Z basis; for qumodes, a shift in the $\hat{x}$ basis. Although this guarantees that even non-Clifford-type *single-variable* errors can be corrected by simple means, it does not yet allow for the correction of *multi-variable* errors including two or more non-commuting variables such as X and Z for qubits, and $\hat{x}$ and $\hat{p}$ for qumodes. Such full QEC codes, however, can be constructed by concatenating a single-variable code using Hadamard and Fourier gates. The first and certainly most famous full QEC code is Shor's nine-qubit code [21]. A qumode version of this code and its experimental realization will be discussed in Chapter 5.

On the level of arbitrary channel (CPTP) maps, the effect of discretization in a QEC protocol can be understood by expanding an arbitrary qubit Kraus operator in the Pauli matrix basis as in Eq. (1.77). Similarly, the WH shift operators serve as a complete basis for arbitrary qumode CPTP maps, see Eq. (1.78). In either case, syndrome detections of Pauli and WH errors will then always remove the offdiagonal terms of the channel output matrix and the remaining terms can be easily corrected. In the qumode case, the reduced error set is, of course, not really discrete. It is, nonetheless, smaller and simpler, containing only phase-space shift errors.

Although universal QEC of *arbitrary, multi-variable* errors occurring on a subset of the physical qubits or qumodes is possible, a subtlety remains when comparing qubit and qumode QEC. This complication arises for the realistic scenario of *multi-channel* errors. Typically, not only a single qubit or qumode will be subject to an error. Usually, every subsystem will be corrupted, and so a hierarchy of errors in terms of the frequency of their occurrence or their size will become important. For instance, as we have seen for qubits, multiple-qubit bit-flip errors may simply be neglected when their probability scales as p^2 compared to the single-qubit error probability p. Similarly, an amplitude damping error may be corrected up to an order $\mathrm{O}(\gamma^2)$ in the damping parameter (see Section 1.4.1 and Chapter 2) [5]. However, for qumodes, amplitude damping becomes a Gaussian channel (see Chapter 2) and, as such, it may simply no longer be correctable when the damping occurs on every encoded qumode in every channel [93]. Nonetheless, whenever a stochastic channel leads to a hierarchy of errors, arbitrary multi-variable, multi-channel

[48] When the signal state $|\psi\rangle = \int \mathrm{d}x \psi(x)|x\rangle$ is a Gaussian state, which is *not* a requirement here.

errors can be suppressed through the standard QEC codes, both for qubits and qumodes [94]. In either case, whether a QEC code is useful at all and whether it is efficient depends on the correctable error set (for instance, the set of arbitrary single-channel errors) and the given channel error model. The only basic assumption typically is that the errors act independently on the individual subsystems.

1.9.2 Stabilizer Codes

A particularly important class of QEC codes is that of so-called stabilizer codes [95, 96], the quantum analogue of classical additive codes. Stabilizer codes are generalizations of stabilizer states. This shall become clear in the present section.

In the DV setting, through an $[N, k]$ stabilizer code, k logical qubits are encoded into N physical qubits. The stabilizer group S, an abelian subgroup of the N-qubit Pauli group[49] with $(N - k)$ stabilizer generators $\langle g_1, g_2, \dots, g_{N-k}\rangle$, defines the codespace which is spanned by the set of simultaneous $+1$ eigenvectors of S. Measuring the $N - k$ stabilizer generators, yielding 2^{N-k} classical syndrome bit values, reveals which orthogonal error subspace an encoded input state is mapped onto. Signal recovery is then achieved by mapping the state back into the codespace with stabilizer eigenvalues $+1$.

Let us illustrate these definitions and notions for the three-qubit code of the preceding section. This code represents a very simple example of a stabilizer code. In this case, $k = 1$ logical qubit is encoded into $N = 3$ physical qubits. The corresponding $[3, 1]$ code is defined through the minimal set of $N - k = 2$ independent stabilizer generators $\langle g_1 \equiv Z \otimes Z \otimes \mathbb{1}, g_2 \equiv \mathbb{1} \otimes Z \otimes Z\rangle$. This set uniquely defines the stabilizer group S for the corresponding stabilizer code with a two-dimensional codespace spanned by $\{|000\rangle, |111\rangle\}$. Since S is abelian, and we have $[g_1, g_2] = 0$, the basis vectors $|000\rangle$ and $|111\rangle$ can be simultaneous eigenvectors of g_1 and g_2 with eigenvalue $+1$.

The effect of the bit-flip channel on the three physical qubits of the repetition code, as described in the preceding section, can now be equivalently expressed in terms of the stabilizers. Up to order $O(p^2)$, including only linear terms in p, we obtain the following stochastic transformations of the stabilizer generators,

$$\begin{aligned}
&\langle Z_1Z_2, Z_2Z_3\rangle \to \langle Z_1Z_2, Z_2Z_3\rangle\,; \quad \text{with probability} && (1-p)^3\,,\\
&\langle Z_1Z_2, Z_2Z_3\rangle \to \langle -Z_1Z_2, Z_2Z_3\rangle\,; && p(1-p)^2\,,\\
&\langle Z_1Z_2, Z_2Z_3\rangle \to \langle -Z_1Z_2, -Z_2Z_3\rangle\,; && p(1-p)^2\,,\\
&\langle Z_1Z_2, Z_2Z_3\rangle \to \langle Z_1Z_2, -Z_2Z_3\rangle\,; && p(1-p)^2\,. \qquad (1.140)
\end{aligned}$$

The first case in the top row corresponds to the no-error case; the encoded state remains in the original codespace. In the other three cases, the encoded state is subject to a bit flip on any one of the three qubits; hence, the encoded state is

[49] Which itself is formed by a tensor product of the one-qubit Pauli group. Recall from footnote 14 on page 19 that we omit all unnecessary prefactors of Pauli operators such as $(\pm i)$.

mapped into one of the orthogonal subspaces $\{X_k|000\rangle, X_k|111\rangle\}$ with $k = 1, 2, 3$. These three error subspaces are each uniquely determined through the new stabilizer generators, as shown in Eq. (1.140), and are each spanned by a new two-dimensional set of simultaneous $+1$ eigenvectors. The syndrome measurement will then reveal the change of the eigenvalues with respect to the original stabilizers, that is, those of the codespace, g_1 and g_2. There are four syndrome outcomes corresponding to the four cases of no error at all ($g_1 = +1, g_2 = +1$), a bit flip on qubit 1 ($g_1 = -1, g_2 = +1$), a bit flip on qubit 2 ($g_1 = -1, g_2 = -1$), and a bit flip on qubit 3 ($g_1 = +1, g_2 = -1$). Thus, measuring the $N - k = 2$ stabilizers of the code uniquely determines the error. Mapping the state from one of the orthogonal error subspaces back into the original codespace enables one to recover an uncorrupted version of the encoded state. This is a general feature of stabilizer codes.

The three-qumode repetition code can be similarly expressed in terms of stabilizers. In this case, we need $N - k = 2$ products of WH operators, $\langle g_1(s) \equiv Z(s) \otimes Z(-s) \otimes \mathbb{1}, g_2(s) \equiv \mathbb{1} \otimes Z(s) \otimes Z(-s)\rangle$, in order to represent the stabilizer group and uniquely define a one-qumode codespace as a subspace of the whole three-qumode space. This infinite-dimensional subspace is spanned by the basis vectors $\{|xxx\rangle | \forall x \in \mathbb{R}\}$, which are simultaneous $+1$ eigenvectors of the stabilizers $g_1(s)$ and $g_2(s)$. More conveniently expressed in terms of the WH generators $\hat{x}$ and $\hat{p}$, we have $N-k = 2$ so-called nullifier conditions, $\hat{x}_1 - \hat{x}_2 = 0$ and $\hat{x}_2 - \hat{x}_3 = 0$ since these combinations must have $\{|xxx\rangle\ | \forall x \in \mathbb{R}\}$ as their simultaneous zero-eigenvectors. The syndrome information now becomes continuous, corresponding to the eigenvalues of $\hat{x}_1 - \hat{x}_2 = u_1$ and $\hat{x}_2 - \hat{x}_3 = u_2$ after an error occurred on any one of the three qumodes. Every pair of these eigenvalues uniquely determines one of the orthogonal error subspaces, $\{X_k(s)|xxx\rangle | \forall x \in \mathbb{R}\}$ with $k = 1, 2, 3$ and $s \in \mathbb{R}$, into which the encoded state is mapped by the channel. Compared with the qubit case in Eq. (1.140), the stabilizer map now becomes

$$\begin{aligned} &\langle Z_1(s) Z_2(-s), Z_2(s) Z_3(-s)\rangle \\ &\to \left\langle \mathrm{e}^{-2\mathrm{i}su_1} Z_1(s) Z_2(-s), \mathrm{e}^{-2\mathrm{i}su_2} Z_2(s) Z_3(-s)\right\rangle , \end{aligned} \tag{1.141}$$

with the syndrome information contained in the phase factors $\mathrm{e}^{-2\mathrm{i}su_1}$ and $\mathrm{e}^{-2\mathrm{i}su_2}$. Though the syndrome is now continuous, the QEC mechanism is very similar to the qubit case; however, the stochastic nature of the qubit channels, as illustrated by Eq. (1.140), will be missing in the most important examples of qumode channels (see Chapter 2).

We have used the notion of stabilizers and stabilizer states already at various times. A stabilizer is a (not necessarily unitary) operator M that, for some vector $|\psi\rangle$, has the property $M|\psi\rangle = |\psi\rangle$. If there is a commuting set of such stabilizers $\{M_i\}$ such that $M_i|\psi\rangle = |\psi\rangle$, $\forall i$, $|\psi\rangle$ may be a unique state vector or an arbitrary vector in a uniquely defined subspace. In fact, the former case is a special case of the latter one.

For instance, for N qubits, $N - k$ Pauli generators will define a 2^k-dimensional subspace $\mathcal{C}$ of the 2^N-dimensional N-qubit space. This subspace $\mathcal{C}$ represents a stabilizer code, and the stabilizer condition becomes $M_i|\psi\rangle = |\psi\rangle$, $\forall i$ and $\forall|\psi\rangle \in \mathcal{C}$. Now, the special case with $k = 0$ means that $\mathcal{C}$ is specified through N Pauli generators. In this case, $\mathcal{C}$ has a dimension such that $M_i|\psi\rangle = |\psi\rangle$, $\forall i$ uniquely defines the rank-1 projector $|\psi\rangle\langle\psi|$ corresponding to a pure N-qubit state. These definitions are similar for qumodes. Later, we shall use full sets of N Pauli and WH stabilizers in order to define multi-party entangled N-qubit and N-qumode graph states, respectively.

Stabilizers and stabilizer codes

stabilizer: any operator M such that $M|\psi\rangle = |\psi\rangle$
stabilizer code: any subspace defined by a commuting stabilizer set $\{M_i\}$
stabilizer state: any such 1-dimensional subspace (pure-state projector)

⊙ **Qubits**

stabilizer codes:
any 2^k-dimensional subspace $\mathcal{C}$ of the 2^N-dimensional N-qubit space defined through $N - k$ Pauli stabilizer generators $\langle g_1, g_2, \ldots, g_{N-k}\rangle$ such that $[g_i, g_j] = 0$ and $g_i|\psi\rangle = |\psi\rangle$, $\forall i, j$ and $\forall|\psi\rangle \in \mathcal{C}$

stabilizer states:
any $2^0 = 1$-dimensional subspace $|\psi\rangle\langle\psi|$ of the 2^N-dimensional N-qubit space defined through N Pauli stabilizer generators $\langle g_1, g_2, \ldots, g_N\rangle$ such that $[g_i, g_j] = 0$ and $g_i|\psi\rangle = |\psi\rangle$, $\forall i, j$

∿∿∿ **Qumodes**

stabilizer codes:
any k-qumode subspace $\mathcal{C}$ of the infinite-dimensional N-qumode space defined through $N - k$ WH stabilizers $\langle g_1(s), g_2(s), \ldots, g_{N-k}(s)\rangle$ such that $[g_i(s), g_j(s)] = 0$ and $g_i(s)|\psi\rangle = |\psi\rangle$, $\forall i, j; s \in \mathbb{R}$, and $\forall|\psi\rangle \in \mathcal{C}$

stabilizer states:
any 1-dimensional subspace $|\psi\rangle\langle\psi|$ of the infinite-dimensional N-qumode space defined through N WH stabilizers $\langle g_1(s), g_2(s), \ldots, g_N(s)\rangle$ such that $[g_i(s), g_j(s)] = 0$ and $g_i(s)|\psi\rangle = |\psi\rangle$, $\forall i, j; s \in \mathbb{R}$

A great advantage of QEC schemes is that they are deterministic which makes them directly applicable to quantum computation. However, this comes at a price. Encoding logical quantum information into a sufficiently large physical system will require expensive resources. Alternatively, probabilistic quantum error detection and, in particular, entanglement purification schemes [22] may be employed in order to reduce the (spatial) resource consumption and the complexity of the quantum circuits for implementing the protocol. This would then be more useful for quantum communication applications, as described in Section 1.7.2. We shall discuss some experimental realizations of QEC and entanglement distillation in Chapter 5.

1.10 Experiment: Non-optical Implementations

Quantum teleportation and quantum information processing were demonstrated in various non-optical implementations. Among these, probably the most prominent and fundamental concept was introduced by Cirac and Zoller for trapped ions [97]. This concept was later extended to other physical systems such as neutral trapped atoms [98] and quantum dots in electromagnetic cavities [99].

The approach by Cirac and Zoller is conceptually related to some of those hybrid protocols which we will discuss in the final chapter of this book. More specifically, the entangling gates between two electronic spin qubits (each defined on two internal energy levels of the ion) are not accomplished through direct interaction, but they are rather mediated by a third "system". In the Cirac–Zoller scheme, this third system is a phononic qubit (defined on two vibrational energy levels of the ion) and it acts as a kind of quantum bus – a so-called *qubus*.

Later, in the quantum optical context, we shall present the notion of optical, hybrid qubus computation, where the qubus is represented by the continuous phase-space variables of a photonic qumode instead of the qubit-subspace of a phononic qumode. An introduction to quantum optical encodings in terms of photonic qubits and qumodes shall be postponed until the following chapter. The motivation of the current section is to at least mention that many of the concepts and protocols discussed so far and applied to quantum optical implementations in the remainder of this book have their counterparts and analogues in implementations that employ non-optically encoded qubit, qumode, and qubus systems using, for instance, nuclear magnetic resonance, superconducting materials, or ion traps.

In this section, we will first explain how to implement a CNOT gate using the Cirac–Zoller scheme, for which we take Schmidt–Kaler's experiment [100] as an example. Then, we shall describe a teleportation experiment by Riebe *et al.* [101] as an example for a possible application.

In Schmidt–Kaler's CNOT-gate experiment, they used $^{40}\mathrm{Ca}^{+}$ ions in a linear Paul trap [100]. The quantum mechanical energy levels are shown in Figure 1.13 [100, 102]. The essence of this scheme is a conditional sign flip operation R_{phase} of the single-ion "computational bases" $(|D,0\rangle, |D,1\rangle, |S,0\rangle, |S,1\rangle)$. More precisely, we have

$$\begin{aligned}
R_{\text{phase}}|D,0\rangle &= |D,0\rangle \ , \\
R_{\text{phase}}|D,1\rangle &= -|D,1\rangle \ , \\
R_{\text{phase}}|S,0\rangle &= -|S,0\rangle \ , \\
R_{\text{phase}}|S,1\rangle &= -|S,1\rangle \ ,
\end{aligned} \tag{1.142}$$

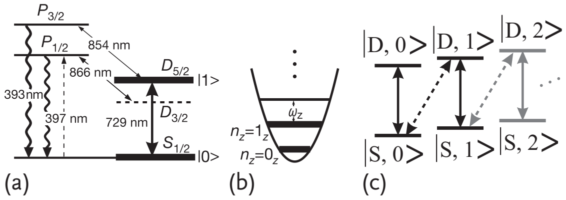

Figure 1.13 Quantum mechanical energy levels of a ^{40}Ca$^+$ ion for quantum information processing [100, 102]. (a) The lower and upper electronic states $S_{1/2}$ $(m = -1/2)$ and $D_{5/2}$ $(m = -1/2)$ of the narrow quadrupole transition at 729 nm provide the two levels to implement a qubit. (b) The lowest two number states, $n_z = 0_z, 1_z$, of the axial vibrational motion in the trap. (c) The combination of electronic states. The notation is |electronic level, vibrational motion number⟩.

where D and S denote the upper and lower electronic levels of a ^{40}Ca$^+$ ion, and 0,1 denotes the quantized number (phonon number) of the vibrational motion of the trapped ions. This is the main trick for realizing the Cirac–Zoller scheme in this system.

The operation R_{phase} can be realized with an effective 2π-pulse on the two-level systems $(|S,0\rangle \leftrightarrow |D,1\rangle)$ and $(|S,1\rangle \leftrightarrow |D,2\rangle)$, changing the sign of all "computational basis" states except for $|D,0\rangle$. Since the Rabi frequency depends on the number of phonons of the trapped ions, we have to use a composite-pulse sequence [103] instead of a single 2π-pulse. More precisely, the operation R_{phase} can be realized through irradiation of four sequential pulses as follows:

$$R_{\text{phase}} = R^+(\pi,0)\,R^+\left(\frac{\pi}{\sqrt{2}},\frac{\pi}{2}\right)R^+(\pi,0)\,R^+\left(\frac{\pi}{\sqrt{2}},\frac{\pi}{2}\right), \tag{1.143}$$

where

$$R^+(\theta,\phi) = \exp\left[\mathrm{i}\frac{\theta}{2}\left(\mathrm{e}^{\mathrm{i}\phi}\sigma^+\hat{b}^\dagger + \mathrm{e}^{-\mathrm{i}\phi}\sigma^-\hat{b}\right)\right]. \tag{1.144}$$

The operator $\sigma^+ = |D\rangle\langle S|$ represents the transition from $|S\rangle$ to $|D\rangle$, and, similarly, $\sigma^- = |S\rangle\langle D|$ that from $|D\rangle$ to $|S\rangle$. The annihilation and creation operators $\hat{b}$ and $\hat{b}^\dagger$, respectively, refer to the phonons in the ion trap and the parameter θ corresponds to the strength and duration of the applied pulse. Finally, ϕ is the relative phase between the optical field and the atomic polarization [102]. Here, the frequency of the optical field for R^+ is blue-shifted from the $|S\rangle - |D\rangle$ transition by a single phonon energy.

One can now verify Eq. (1.142) by using Eqs. (1.143) and (1.144). For example,

$$\begin{aligned}R_{\text{phase}}|S,0\rangle &= R^+(\pi,0)\,R^+\left(\frac{\pi}{\sqrt{2}},\frac{\pi}{2}\right)R^+(\pi,0)\,R^+\left(\frac{\pi}{\sqrt{2}},\frac{\pi}{2}\right)|S,0\rangle\\ &= R^+(\pi,0)\,R^+\left(\frac{\pi}{\sqrt{2}},\frac{\pi}{2}\right)R^+(\pi,0)\\ &\quad\times\left(\cos\frac{\pi}{2\sqrt{2}}|S,0\rangle - \sin\frac{\pi}{2\sqrt{2}}|D,1\rangle\right)\end{aligned}$$

$$
\begin{aligned}
&= R^{+}(\pi, 0) R^{+}\left(\frac{\pi}{\sqrt{2}}, \frac{\pi}{2}\right) \\
&\quad \times \left(\mathrm{i}\cos\frac{\pi}{2\sqrt{2}}|D,1\rangle - \mathrm{i}\sin\frac{\pi}{2\sqrt{2}}|S,0\rangle\right) \\
&= R^{+}(\pi, 0)\left[\mathrm{i}\cos\frac{\pi}{2\sqrt{2}}\left(\cos\frac{\pi}{2\sqrt{2}}|D,1\rangle + \sin\frac{\pi}{2\sqrt{2}}|S,0\rangle\right)\right. \\
&\quad \left. -\mathrm{i}\sin\frac{\pi}{2\sqrt{2}}\left(\cos\frac{\pi}{2\sqrt{2}}|S,0\rangle - \sin\frac{\pi}{2\sqrt{2}}|D,1\rangle\right)\right] \\
&= \mathrm{i}R^{+}(\pi, 0)|D,1\rangle \\
&= -|S,0\rangle. \qquad (1.145)
\end{aligned}
$$

By using the R_{phase}, we can build a CNOT gate R_{CNOT} for the single-ion "computational bases", that is,

$$R_{\text{CNOT}} = R\left(\frac{\pi}{2}, -\frac{\pi}{2}\right) R_{\text{phase}} R\left(\frac{\pi}{2}, \frac{\pi}{2}\right), \qquad (1.146)$$

where

$$R(\theta, \phi) = \exp\left[\mathrm{i}\frac{\theta}{2}\left(\mathrm{e}^{\mathrm{i}\phi}\sigma^{+} + \mathrm{e}^{-\mathrm{i}\phi}\sigma^{-}\right)\right], \qquad (1.147)$$

and the $R(\theta, \phi)$ transformation can be realized with a pulse irradiation on resonance with the $|S\rangle - |D\rangle$ transition. The CNOT gate transforms the single-ion "computational bases" as follows:

$$
\begin{aligned}
R_{\text{CNOT}}|S,0\rangle &= -|D,0\rangle\ , \\
R_{\text{CNOT}}|S,1\rangle &= -|S,1\rangle\ , \\
R_{\text{CNOT}}|D,0\rangle &= -|S,0\rangle\ , \\
R_{\text{CNOT}}|D,1\rangle &= -|D,1\rangle\ , \qquad (1.148)
\end{aligned}
$$

where the phonon numbers $n = 0$ and $n = 1$ correspond to a logical bit of one and zero, respectively. These relations can be checked using Eq. (1.147). For example,

$$
\begin{aligned}
R_{\text{CNOT}}|S,0\rangle &= R\left(\frac{\pi}{2}, -\frac{\pi}{2}\right) R_{\text{phase}} R\left(\frac{\pi}{2}, \frac{\pi}{2}\right)|S,0\rangle \\
&= R\left(\frac{\pi}{2}, -\frac{\pi}{2}\right) R_{\text{phase}}\left(\cos\frac{\pi}{4}|S,0\rangle + \sin\frac{\pi}{4}|D,0\rangle\right) \\
&= R\left(\frac{\pi}{2}, -\frac{\pi}{2}\right)\left(-\cos\frac{\pi}{4}|S,0\rangle - \sin\frac{\pi}{4}|D,0\rangle\right) \\
&= -\cos\frac{\pi}{4}\left(\cos\frac{\pi}{4}|S,0\rangle + \sin\frac{\pi}{4}|D,0\rangle\right) \\
&\quad - \sin\frac{\pi}{4}\left(\cos\frac{\pi}{4}|D,0\rangle - \sin\frac{\pi}{4}|S,0\rangle\right) \\
&= -|D,0\rangle\ . \qquad (1.149)
\end{aligned}
$$

Finally, we can construct a CNOT gate for two ions $|\text{ion1, ion2}\rangle = |\text{control, target}\rangle$, where the logical zero and one are encoded into the S and D levels of the ions, respectively. First, quantum information encoded into the electronic levels of the *control* ion is transferred onto the phonon levels (i.e., the vibrational qubit encoded into the qubus mode) through the $R_c^+(\pi,0)$ operation[50] (pulse irradiation) as follows:

$$\begin{aligned} R_c^+(\pi,0)(\alpha|S,0\rangle + \beta|D,0\rangle) &= \mathrm{i}\alpha|D,1\rangle + \beta|D,0\rangle \\ &= |D\rangle \otimes (\mathrm{i}\alpha|1\rangle + \beta|0\rangle) \,, \end{aligned} \tag{1.150}$$

where the phonon number is initially zero and we use the definition of R^+ in Eq. (1.144). Then, the single-ion CNOT operation R_{CNOT} is performed on the *target* ion. When the target ion is in the $|S\rangle$ state, the CNOT operation transforms the state as follows:

$$R_{\mathrm{CNOT}}(\mathrm{i}\alpha|S,1\rangle + \beta|S,0\rangle) = -\mathrm{i}\alpha|S,1\rangle - \beta|D,0\rangle \,, \tag{1.151}$$

using Eq. (1.148). As a final step, the $R_c^+(\pi,0)$ operation is applied to the *control* ion again. With this operation, the state of the control ion, whose electronic state is $|D\rangle$ as in Eq. (1.150), is transformed as follows:

$$\begin{aligned} R_c^+(\pi,0)(-\mathrm{i}\alpha|D,S,1\rangle - \beta|D,D,0\rangle) &= -\mathrm{i}\alpha(-\mathrm{i}|S,S,0\rangle) - \beta|D,D,0\rangle \\ &= -(\alpha|S,S\rangle + \beta|D,D\rangle) \otimes |0\rangle \,, \end{aligned} \tag{1.152}$$

with the notation |control, target, phonon number⟩. Similarly, we obtain the result for the case with $|D\rangle$ as the initial target-ion's state. Overall we have the following input-output relation for the CNOT gate acting on a two-ion state |control, target⟩:

$$\begin{aligned} &|S,S\rangle \to -|S,S\rangle \,, \\ &|S,D\rangle \to -|S,D\rangle \,, \\ &|D,S\rangle \to -|D,D\rangle \,, \\ &|D,D\rangle \to -|D,S\rangle \,, \end{aligned} \tag{1.153}$$

corresponding to a CNOT operation for the logical states $|S\rangle = |0\rangle$ and $|D\rangle = |1\rangle$. Moreover, the result of Eq. (1.152) means that one can create an entangled state of two ions using this CNOT operation.

Figure 1.14 shows the experimental results of the CNOT gate performed by Schmidt–Kaler *et al.* [100]. From the results, one can see that Eq. (1.153) is very well experimentally verified. Schmidt–Kaler *et al.* also performed the CNOT experiment for a $|S+D,S\rangle$ input. Figure 1.15 shows the corresponding results. In this case, only the states $|S,S\rangle$ and $|D,D\rangle$ are observed with a probability of about 0.5. Phase coherence was also verified by applying an additional $\pi/2$ pulse on the $|S,0\rangle - |D,0\rangle$ transition followed by a projective measurement [100].

Now, we will turn to a discussion of the experiments for quantum teleportation between trapped ions performed by Riebe *et al.* [101].

[50] The subscript c denotes the operation on the control ion.

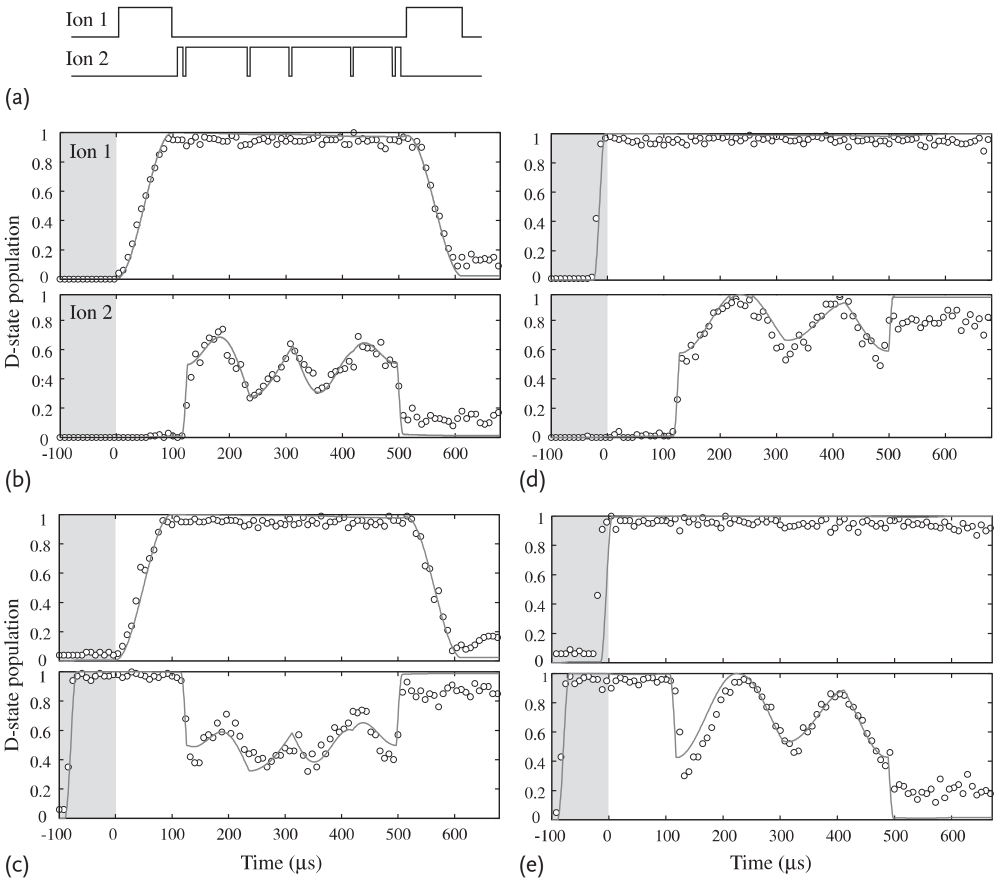

Figure 1.14 State evolution of $|\text{control}, \text{target}\rangle = |\text{ion1}, \text{ion2}\rangle$ under the CNOT operation [100]. First, the ions are initialized in the states (b) $|S, S\rangle$, (c) $|S, D\rangle$, (d) $|D, S\rangle$, or (e) $|D, D\rangle$ (shaded area, $t \leq 0$). Then, the quantum-gate pulse sequence (a) is applied: (i) quantum information encoded in the electronic levels of the *control* ion is transferred to the phonon levels (qubus mode) through $R_c^+(\pi, 0)$, (ii) the single-ion CNOT operation R_{CNOT} is applied to the *target* ion, (iii) the $R_c^+(\pi, 0)$ operation is performed on the *control* ion again.

Figure 1.16 shows the quantum circuit for teleportation from ion 1 to ion 3 [101]. This circuit is realized using the same system ($^{40}\text{Ca}^+$) and techniques (pulse irradiation) explained above for the CNOT gate. The pulse sequence for teleportation is summarized in Table 1.1 [101]. First, ion 2 and ion 3 are prepared in the Bell state $|\Psi^+\rangle_{23} = (|0\rangle_2|1\rangle_3 + |1\rangle_2|0\rangle_3)/\sqrt{2}$, the lifetime of which exceeds 100 ms.

Then, at any time within this lifetime, the actual teleportation step can be carried out: ion 1 is prepared in an arbitrary input state through local rotations. In Riebe's experiment, the input state $|\psi_{\text{in}}\rangle$ was drawn from a set of four non-orthogonal test states, $\{|1\rangle, |0\rangle, (|0\rangle + |1\rangle)/\sqrt{2}, (i|0\rangle + |1\rangle)/\sqrt{2}\}$. The Bell measurement is per-

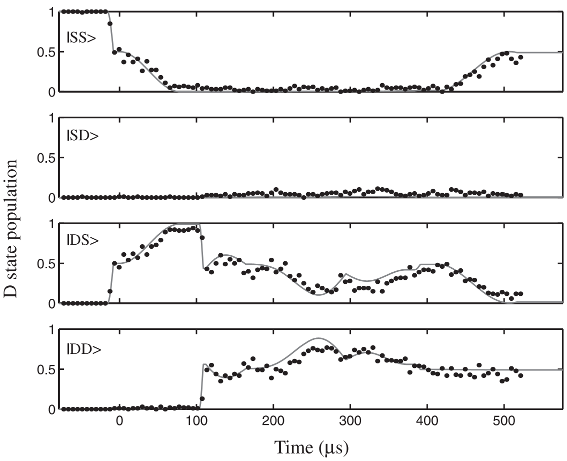

Figure 1.15 The CNOT operation for a $|S+D, S\rangle$ input [100].

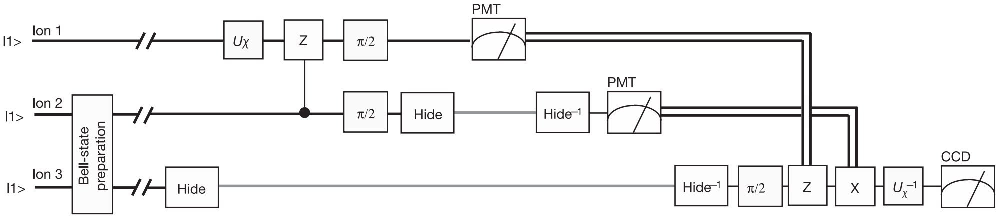

Figure 1.16 Quantum circuit for teleportation from ion 1 to ion 3 [101]. The state to be teleported (input state) is encoded in ion 1 by the operation U_x. The Bell measurement is performed through a controlled Z-gate (phase gate) followed by π/2 rotations and state detections of ions 1 and 2. This implementation uses a Bell basis rotated by π/4 with respect to the standard convention. Therefore, a π/2 rotation on ion 3 is required before the final reconstruction operations Z and X. Grey lines indicate qubits that are protected against light scattering. Ions 1 and 2 are detected by observing their fluorescence on a photomultiplier tube (PMT). For the fidelity analysis, U_x^{-1} is applied to ion 3 and its quantum state is measured by resonance fluorescence using a CCD camera. Here, the initial state is $|1\rangle = |S\rangle$ (different from the CNOT-gate experiment where the initial state is $|0\rangle$).

formed by means of a controlled Z-gate (phase gate) followed by π/2 rotations and state detections of ions 1 and 2, where the state detection is achieved by fluorescence detection from the $S_{1/2}$ state (logical $|1\rangle$) with a photomultiplier tube (PMT). Conditioned upon the measurement results, if necessary, an appropriate unitary qubit rotation, $-i\sigma_y, -i\sigma_z, i\sigma_x$, is applied in order to recreate the input state in ion 3.

Figure 1.17 shows the results of the teleportation experiment. Here, the fidelities between the input and the output $\langle\psi_{\text{in}}|\hat{\rho}_{\text{out}}|\psi_{\text{in}}\rangle$ are shown. Whenever the fidelity exceeds the classical boundary of 2/3, quantum teleportation is successful. The fidelities of Figure 1.17 are clearly higher than 2/3 for any inputs, thus confirming successful quantum teleportation. The fidelities for the output state without the

Table 1.1 Pulse sequence for teleportation from ion 1 to ion 3 [101]. Here, the superscript *C* denotes the carrier transition with no change of the motional states (phonon numbers). The corresponding operations are the same as before without the superscript for the CNOT gate. The superscript *H* denotes the carrier transition from the $S_{1/2}$ $(m = -1/2)$ to the $D_{5/2}$ $(m = -5/2)$ level in the Zeeman manifold.

	Action	Comment
1	Light at 397 nm	Doppler preparation
2	Light at 729 nm	Sideband cooling
3	Light at 397 nm	Optical pumping
		Entangle
4	$R_3^{+}(\pi/2, 3\pi/2)$	Entangle ion 3 with motional qubit
5	$R_2^{\mathrm{C}}(\pi, 3\pi/2)$	Prepare ion 2 for entanglement
6	$R_2^{+}(\pi, \pi/2)$	Entangle ion 2 with ion 3
7	Wait for 1 µS–10 000 µS	Standby for teleportation
8	$R_3^{\mathrm{H}}(\pi, 0)$	Hide target ion
9	$R_1^{\mathrm{C}}(\vartheta_x, \varphi_x)$	Prepare source ion 1 in state x
		Rotate into Bell basis
10	$R_2^{+}(\pi, 3\pi/2)$	Get motional qubit from ion 2
11	$R_1^{+}(\pi/\sqrt{2}, \pi/2)$	Composite pulse for phase gate
12	$R_1^{+}(\pi, 0)$	Composite pulse for phase gate
13	$R_1^{+}(\pi/\sqrt{2}, \pi/2)$	Composite pulse for phase gate
14	$R_1^{+}(\pi, 0)$	Composite pulse for phase gate
15	$R_1^{\mathrm{C}}(\pi, \pi/2)$	Spin echo on ion 1
16	$R_3^{\mathrm{H}}(\pi, \pi)$	Unhide ion 3 for spin echo
17	$R_3^{\mathrm{C}}(\pi, \pi/2)$	Spin echo on ion 3
18	$R_3^{\mathrm{H}}(\pi, 0)$	Hide ion 3 again
19	$R_2^{+}(\pi, \pi/2)$	Write motional qubit back to ion 2
20	$R_1^{\mathrm{C}}(\pi/2, 3\pi/2)$	Part of rotation into Bell basis
21	$R_2^{\mathrm{C}}(\pi/2, \pi/2)$	Finalize rotation into Bell basis
		Read out
22	$R_2^{\mathrm{H}}(\pi, 0)$	Hide ion 2
23	PM Detection for 250 µs	Read out of ion 1 with photomultiplier
24	$R_1^{\mathrm{H}}(\pi, 0)$	Hide ion 1
25	$R_2^{\mathrm{H}}(\pi, \pi)$	Unhide ion 2
26	PM Detection for 250 µs	Read out of ion 2 with photomultiplier
27	$R_2^{\mathrm{H}}(\pi, 0)$	Hide ion 2
28	Wait 300 µs	Let system rephase; part of spin echo
29	$R_3^{\mathrm{H}}(\pi, \pi)$	Unhide ion 3
30	$R_3^{\mathrm{C}}(\pi/2, 3\pi/2 + \phi)$	Change basis
		Reconstruction
31	$R_3^{\mathrm{C}}(\pi, \phi)$	$\mathrm{i}\sigma_x = -\mathrm{i}\sigma_z$ conditioned on PM detection 1
32	$R_3^{\mathrm{C}}(\pi, \pi/2 + \phi)$	$-\mathrm{i}\sigma_y = -\mathrm{i}\sigma_z$ conditioned on PM detection 1
33	$R_3^{\mathrm{C}}(\pi, \phi)$	$\mathrm{i}\sigma_x$ conditioned on PM detection 2
34	$R_3^{\mathrm{C}}(\vartheta_x, \varphi_x + \pi + \phi)$	Inverse of preparation of x with offset ϕ
35	Light at 397 nm	Read out of ion 3 with camera

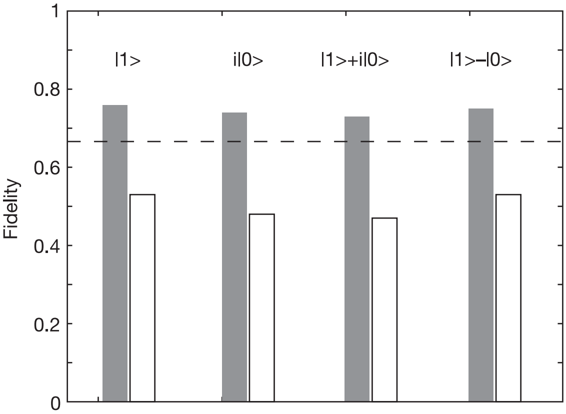

Figure 1.17 Results of the teleportation experiment [100]. The classical boundary of the teleportation fidelity (2/3) is shown by the dashed line. The gray bars correspond to the results obtained in quantum teleportation and the white bars are the results when the reconstruction operations are omitted.

final reconstruction operations are also shown in Figure 1.17. In this case, no more than 1/2 should be obtained for the fidelity and indeed the experimental value was 49.6%.

In the following chapter, an introduction to optical quantum information processing is presented. Most of those concepts, tools, and protocols presented thus far will turn out to have their specific manifestation in the language of quantum optics.