# 7

# Applications to quantum information processing

## 7.1 Introduction

Any technology that functions at the quantum level must face the issues of measurement and control. We have good reasons to believe that quantum physics enables communication and computation tasks that are either impossible or intractable in a classical world [NC00]. The security of widely used classical cryptographic systems relies upon the difficulty of certain computational tasks, such as breaking large semi-prime numbers into their two prime factors in the case of RSA encryption. By contrast, quantum cryptography can be *absolutely* secure, and is already a commercial reality. At the same time, the prospect of a quantum computer vastly faster than any classical computer at certain tasks is driving an international research programme to implement quantum information processing. Shor's factoring algorithm would enable a quantum computer to find factors exponentially faster than any known algorithm for classical computers, making classical encryption insecure. In this chapter, we investigate how issues of measurement and control arise in this most challenging quantum technology of all, quantum computation.

The subjects of information theory and computational theory at first sight appear to belong to mathematics rather than physics. For example, communication was thought to have been captured by Shannon's abstract theory of information [SW49, Sha49]. However, physics must impact on such fundamental concepts once we acknowledge the fact that information requires a physical medium to support it. This is a rather obvious point; so obvious, in fact, that it was only recently realized that the conventional mathematics of information and computation are based on an implicit classical intuition about the physical world. This intuition unnecessarily constrains our view of what tasks are tractable or even possible.

Shannon's theory of information and communication was thoroughly grounded in classical physics. He assumed that the fundamental unit of information is a classical 'bit', which is definitely either in state 'zero' or in state 'one', and that the process of sending bits through channels could be described in an entirely classical way. This focus on the classical had important practical implications. For example, in 1949 Shannon used his formulation of information theory to 'prove' [Sha49] that it is impossible for two parties to communicate with perfect privacy, unless they have pre-shared a random key as long as the message they wish to communicate.

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

Insofar as Shannon's theory is concerned, any physical quantity that can take one of two distinct values can support a bit. One physical instantiation of a bit is as good as any other – we might say that bits are *fungible*. Clearly, bits can exist in a quantum world. There are many quantum systems that are adequate to the task: spin of a nucleus, polarization of a photon, any two stationary states of an atom etc., but, as the reader well knows, there is a big difference between a classical bit and a two-level quantum system: the latter can be in an arbitrary *superposition* of its two levels.

One might think that such a superposition is not so different from a classical bit in a mixture, describing a lack of certainty as to whether it is in state zero or one, but actually the situations are quite different. The entropy of the classical state corresponding to an uncertain bit value is non-zero, whereas the entropy of a pure quantum superposition state is zero. To capture this difference, Schumacher coined the term *qubit* for a quantum bit [Sch95]. Like bits, qubits are fungible and we can develop quantum information theory without referring to any particular physical implementation. This theory seeks to establish abstract principles for communication and computational tasks when information is encoded in qubits. For a thorough introduction to this subject we refer the reader to the book by Nielsen and Chuang [NC00].

It will help in what follows to state a few definitions. In writing the state of a qubit, we typically use some preferred orthonormal basis, which, as in Chapter 1, we denote $\{|0\rangle, |1\rangle\}$ and call the *logical basis* or *computational basis*. The qubit Hilbert space could be the entire Hilbert space of the system or just a two-dimensional subspace of the total Hilbert space. In physical terms, the logical basis is determined by criteria such as ease of preparation, ease of measurement and isolation from sources of decoherence (as in the pointer basis of Section 3.7). For example, if the qubit is represented by a spin of a spin-half particle in a static magnetic field, it is convenient to regard the computational basis as the eigenstates of the component of spin in the direction of the field, since the spin-up state can be prepared to a good approximation by allowing the system to come to thermal equilibrium in a large enough magnetic field. If the physical system is a mesoscopic superconducting system (see Section 3.10.2), the computational basis could be two distinct charge states on a superconducting island, or two distinct phase states, or some basis in between these. A charge qubit is very difficult to isolate from the environment and thus it may be preferable to use the phase basis. On the other hand, single electronics can make the measurement of charge particularly easy. In all of these cases the qubit Hilbert space is only a two-dimensional subspace of an infinite-dimensional Hilbert space describing the superconducting system.

Once the logical basis has been fixed, we can specify three Pauli operators, $X$, $Y$ and $Z$, by their action on the logical states $|z\rangle$, $z \in \{0, 1\}$:

$$Z|z\rangle = (-1)^z|z\rangle, \tag{7.1}$$

$$Y|z\rangle = \mathrm{i}(-1)^z|1-z\rangle, \tag{7.2}$$

$$X|z\rangle = |1-z\rangle. \tag{7.3}$$

Here, we are following the convention common in the field of quantum information [NC00]. Note the different notation from what we have used previously (see Box 3.1) of $\hat{\sigma}_x$, $\hat{\sigma}_y$ and $\hat{\sigma}_z$. In particular, here we do not put hats on $X$, $Y$ and $Z$, even though they are operators. When in this chapter we do use $\hat{X}$ and $\hat{Y}$, these indicate operators with continuous spectra, as in earlier chapters. Another convention is to omit the tensor product between Pauli operators. Thus, for a two-qubit system, $ZX$ means $Z \otimes X$. Note that the square of any Pauli operator is unity, which we denote $I$.

This chapter is structured as follows. Section 7.2 introduces a widely used primitive of quantum information processing: teleportation of a qubit. This involves discrete (in time) measurement and feedforward. In Section 7.3, we consider the analogous protocol for variables with continuous spectra. In Section 7.4, we introduce the basic ideas of quantum errors, and how to protect against them by quantum encoding and error correction. In Section 7.5 we relate error correction to the quantum feedback control of Chapter 5 by considering continuously detected errors. In Section 7.6 we consider the conventional error model (i.e. undetected errors), but formulate the error correction as a control problem with continuous measurement and Hamiltonian feedback. In Section 7.7 we consider the same problem (continuous error correction) but without an explicit measurement step; that is, we treat the measurement and control apparatus as a physical system composed of a small number of qubits. In Section 7.8 we turn to quantum computing, and show that discrete measurement and control techniques can be used to engineer quantum logic gates in an optical system where the carriers of the quantum information (photons) do not interact. In Section 7.9, we show that this idea, called linear optical quantum computation, can be augmented using techniques from continuous measurement and control. In particular, adaptive phase measurements allow one to create, and perform quantum logic operations upon, qubits comprising arbitrary superpositions of zero and one photon. We conclude as usual with suggestions for further reading.

## 7.2 Quantum teleportation of a qubit

We begin with one of the protocols that set the ball rolling in quantum information: quantum teleportation of a qubit [BBC$^+$93]. This task explicitly involves both quantum measurement and control. It also requires an entangled state, which is shared by two parties, the sender and the receiver. The sender, Alice, using only classical communication, must send an unknown qubit state to a distant receiver, Bob. She can do this in such a way that neither of them learns anything about the state of the qubit. The protocol is called teleportation because the overall result is that the qubit is transferred from Alice to Bob even though there is no physical transportation of any quantum system from Alice to Bob. It is illustrated in Fig. 7.1 by a *quantum circuit diagram*, the first of many in this chapter.

### 7.2.1 The protocol

The key resource (which is consumed) in this quantum teleportation protocol is the bipartite entangled state. Alice and Bob initially each have one qubit of a two-qubit maximally

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

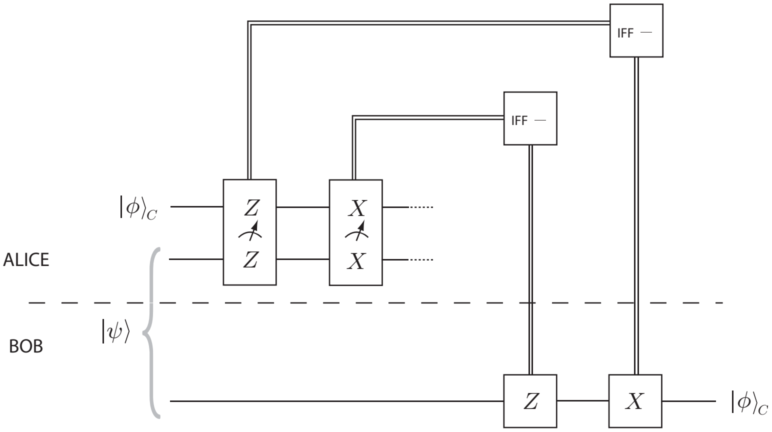

Fig. 7.1 A quantum circuit diagram for quantum teleportation of an arbitrary qubit state $|\phi\rangle_C$ from Alice to Bob, using an entangled Bell state $|\psi\rangle$ shared by Alice and Bob. The single lines represent quantum information in qubits, with time increasing from left to right. The two boxes containing dials represent a measurement of the operator contained within ($ZZ$ and $XX$, respectively), with possible outcomes ±1. The double lines represent classical bits: the outcomes of the measurements and the controls which implement (or not) the quantum gates $X$ and $Z$, respectively. For details see the text.

entangled state such as

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B). \tag{7.4}$$

This is often known as a Bell state, because of the important role such states play in Bell's theorem [Bel64] (see Section 1.2.1). In addition, Alice has in her possession another qubit, which we will refer to as the *client*, prepared in an arbitrary state (it could even be entangled with other systems). For ease of presentation, we will assume that the client qubit is in a pure state

$$|\phi\rangle_C = \alpha|0\rangle_C + \beta|1\rangle_C. \tag{7.5}$$

This state is unknown to Alice and Bob; it is known only to the client who has entrusted it to Alice for delivery to Bob. The total state of the three systems is then

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle_C + \beta|1\rangle_C)(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B). \tag{7.6}$$

At this stage of the protocol, Alice has at her location two qubits, the client qubit, in an unknown (to her) state, and one of an entangled pair of qubits. The other entangled qubit is held at a distant location by Bob.

The next stage requires Alice to measure two physical quantities, represented by commuting operators, on her two qubits. These quantities are joint properties of her two qubits, with operators $Z_A \otimes Z_C$ and $X_A \otimes X_C$.

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

**Exercise 7.1** *Show that these operators commute, that they both have eigenvalues* ±1 *and that the simultaneous eigenstates are*

$$\sqrt{2}|+;+\rangle = |00\rangle + |11\rangle, \tag{7.7}$$

$$\sqrt{2}|+;-\rangle = |00\rangle - |11\rangle, \tag{7.8}$$

$$\sqrt{2}|-;+\rangle = |01\rangle + |10\rangle, \tag{7.9}$$

$$\sqrt{2}|-;-\rangle = |01\rangle - |10\rangle. \tag{7.10}$$

*Here the first* ± *label refers to the eigenvalue for $ZZ$ and the second* ± *label to the eigenvalue of $XX$, and the order of the qubits is $AC$ as above.*

This is known as a Bell measurement, because the above eigenstates are Bell states.

On rewriting the state of the three qubits, Eq. (7.6), in terms of these eigenstates for qubits $A$ and $C$, we find

$$\begin{aligned}|\Psi\rangle = \frac{1}{2}[&|+;+\rangle(\alpha|0\rangle_B + \beta|1\rangle_B) + |+;-\rangle(\alpha|0\rangle_B - \beta|1\rangle)\\ &+|-;+\rangle(\alpha|1\rangle_B + \beta|0\rangle_B) + |-;-\rangle(-\alpha|1\rangle_B + \beta|0\rangle_B)].\end{aligned} \tag{7.11}$$

**Exercise 7.2** *Verify this.*

Remember that $|+;+\rangle$ etc. refer to entangled states of the $A$ and $C$ qubits held locally by Alice. It is now clear that the four possible results for the two joint measurements that Alice must make are equally probable. The results of Alice's measurement thus give two bits of information. Furthermore, we can simply read off the conditional state of Bob's qubit. For example, if Alice obtains the result $(+;+)$ then Bob's qubit must be in the state $|\phi\rangle_B$. That is, it is in the same state as the original client qubit held by Alice. Of course, until Bob knows the outcome of Alice's measurement he cannot describe the state of his qubit in this way. Meanwhile Alice's final state is unrelated to the original state of the client qubit because the Bell measurement is a *complete* measurement (see Section 1.4.2).

The final step of the protocol requires Alice to send the results of her measurements to Bob by *classical communication* (e.g. telephone or email). Once Bob has this information, he may, using a local unitary transformation conditional on Alice's results, transform his qubit into the same state as the original client qubit held by Alice. As we have seen, if Alice gets the result $(+;+)$, then Bob need do nothing. If Alice gets the result $(-;+)$, then Bob, upon receiving this information, should act upon his local system with the unitary transformation $X_B$ to change his state into $|\phi\rangle_B$. Similarly, if Alice gets $(+;-)$ then Bob should act with $Z_B$, and if $(-;-)$, then with $Y_B \propto Z_B X_B$. At no time does Alice or Bob learn anything about the state of the client system; as shown above, the results of Alice's measurement are completely random. Note also that the communication from Alice to Bob is limited to the speed of light, so the teleportation protocol does not transfer the quantum state faster than light.

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

**Exercise 7.3** *Suppose the client state is itself entangled with another system, Q. Convince yourself that, after teleportation, this will result in Bob's qubit being entangled in the same way with Q.*

Clearly the teleportation protocol just described is just a rather simple form of measurement-based control in which the results of measurement upon a part of the total system are used to effect a local unitary transformation on another part of the system. While Alice and Bob share entangled qubits they must always be regarded as acting on a single quantum system, no matter how distant they are in space. Only at the end of the protocol can Bob's qubit be regarded as an independent quantum system.

### 7.2.2 A criterion for demonstrating qubit teleportation

In any real experiment, every part of the teleportation will be imperfect: the preparation of the entanglement resource, Alice's measurement and Bob's control. As a result, the teleportation will not work perfectly, so Bob will end up with a state $\rho$ different from the desired state $|\phi\rangle\langle\phi|$. The quality of the teleportation can be quantified by the *fidelity*,

$$F = \langle\phi|\rho|\phi\rangle, \tag{7.12}$$

which is the probability for the client to find Bob's system in the desired state $|\phi\rangle$, if he were to check.

**Exercise 7.4** *Show that* $F = 1$ *iff* $\rho = |\phi\rangle\langle\phi|$.

How much less than unity can the fidelity be before we stop calling this process *quantum* teleportation? To turn the question around, what is the maximum fidelity that can be obtained without using a quantum resource (i.e. an entangled state).

It turns out that the answer to this question hangs on what it means to say that the client state is *unknown* to Alice and Bob. One answer to this question has been given by Braunstein *et al.* [BFK00] by specifying the ensemble from which client states are drawn. To make Alice's and Bob's task as difficult as possible, we take the ensemble to weight all pure states equally.

**Exercise 7.5** *Convince yourself that the task of Alice and Bob is easier if any other ensemble is chosen. In particular, if the ensemble comprises two orthogonal states (known to Alice and Bob), show that they can achieve a fidelity of unity without any shared entangled state.*

We may parameterize qubit states on the Bloch sphere (see Box 3.1) by $\Omega = (\theta, \phi)$ according to

$$|\Omega\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \mathrm{e}^{\mathrm{i}\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle. \tag{7.13}$$

The uniform ensemble of pure states then has the probability distribution $[1/(4\pi)]\mathrm{d}\Omega = [1/(4\pi)]\mathrm{d}\phi \sin\theta\, \mathrm{d}\theta$.

For this ensemble, there are various ways of achieving the best possible classical teleportation (that is, without using entanglement). One way is for Alice to measure $Z_A$ and tell Bob the result, and for Bob to prepare the corresponding eigenstate. From Eq. (7.13), the probabilities for Alice to obtain the results ±1 are $\cos^2(\theta/2)$ and $\sin^2(\theta/2)$, respectively. Thus, the state that Bob will reconstruct is, on average,

$$\rho_\Omega = \cos^2\left(\frac{\theta}{2}\right)|0\rangle\langle 0| + \sin^2\left(\frac{\theta}{2}\right)|1\rangle\langle 1|. \tag{7.14}$$

**Exercise 7.6** *Show that the same state results if Alice and Bob follow the quantum teleportation protocol specified in Section 7.2.1, but with their entangled state $|\psi\rangle$ replaced by the classically correlated state*

$$\rho_{AB} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|). \tag{7.15}$$

From Eq. (7.14), the *average fidelity* for the teleportation is

$$\bar{F} = \int \frac{\mathrm{d}\Omega}{4\pi}\langle\Omega|\rho_\Omega|\Omega\rangle. \tag{7.16}$$

**Exercise 7.7** *Show that this integral evaluates to* $2/3$.

Thus if, in a series of experimental runs, we find an average fidelity greater than 0.67, we can be confident that some degree of entanglement was present in the resource used and that the protocol used was indeed quantum. This has now been demonstrated in a number of different experimental settings, perhaps most convincingly using trapped-ion qubits, with Wineland's group achieving a fidelity of 0.78 [BCS$^+$04].

As it stands, teleporting qubits, while certainly a fascinating aspect of quantum information theory, does not seem enormously useful. After all, it requires shared entanglement, which requires a quantum channel between the two parties to set up. If that quantum channel can be kept open then it would be far easier to send the qubit directly down that channel, rather than teleporting it. However, we will see in Section 7.8.3 that quantum teleportation has an essential role in the field of measurement-based quantum computing.

## 7.3 Quantum teleportation for continuous variables

Entangled qubit states are a particularly simple way to see how teleportation works. However, we can devise a teleportation protocol for quantum systems of any dimension, even infinite-dimensional ones. In fact, the infinite-dimensional case is also simple to treat [Vai94], and has also been demonstrated experimentally [FSB$^+$98]. It is usually referred to as continuous-variable (CV) quantum teleportation, because operators with continuous spectra play a key role in the protocol. As noted in the introduction, here we denote such operators as $\hat{X}$ or $\hat{Y}$, with the hats to differentiate these from Pauli operators.

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

### 7.3.1 The ideal protocol

The basic procedure is the same as in the qubit case. Alice has an unknown (infinite-dimensional) client state $|\phi\rangle_C$ and she shares with Bob an entangled state $|\psi\rangle_{AB}$. For perfect teleportation of an arbitrary state $|\phi\rangle_C$, the state $|\psi\rangle_{AB}$ must contain an infinite amount of entanglement (see Section A.2.2). Let us define CV quadrature operators $\hat{X}_A$ and $\hat{Y}_A$ for Alice, and similarly for Bob and for the client. These obey

$$[\hat{X}_\nu, \hat{Y}_\mu] = 2\mathrm{i}\delta_{\nu,\mu} \text{ for } \nu, \mu \in \{A, B, C\}, \tag{7.17}$$

and are assumed to form a complete set of observables (see Section 6.6). This allows us to define a particularly convenient choice of entangled state for Alice and Bob:

$$|\psi\rangle_{AB} = \mathrm{e}^{-\mathrm{i}\hat{Y}_A\hat{X}_B/2}|X := X_0\rangle_A|Y := Y_0\rangle_B. \tag{7.18}$$

Here we are following our usual convention so that $|X := X_0\rangle_A$ is the eigenstate of $\hat{X}_A$ with eigenvalue $X_0$ etc.

**Exercise 7.8** *Show that $|\psi\rangle_{AB}$ is a joint eigenstate of $\hat{X}_A - \hat{X}_B$ and $\hat{Y}_A + \hat{Y}_B$, with eigenvalues $X_0$ and $Y_0$.*
**Hint:** *First show that $\mathrm{e}^{\mathrm{i}\hat{Y}_A\hat{X}_B/2}\hat{X}_A\mathrm{e}^{-\mathrm{i}\hat{Y}_A\hat{X}_B/2} = \hat{X}_A + \hat{X}_B$, using Eq. (2.109).*

For the case $X_0 = Y_0 = 0$ (as we will assume below), this state is known as an EPR state, because it was first introduced in the famous paper by Einstein, Podolsky and Rosen [EPR35]. Note that the entanglement in this state is also manifest in correlations between other pairs of observables, such as number and phase [MB99].

In the protocol for teleportation based on this state, Alice now makes joint measurements of $\hat{X}_C - \hat{X}_A$ and $\hat{Y}_C + \hat{Y}_A$ on the two systems in her possession. This yields two real numbers, $X$ and $Y$, respectively. The conditional state resulting from this joint quadrature measurement is described by the projection onto the state $\mathrm{e}^{-\mathrm{i}\hat{Y}_C\hat{X}_A/2}|X\rangle_C|Y\rangle_A$. Thus the conditioned state of Bob's system is

$$|\phi^{XY}\rangle_B \propto {}_C\langle X|_A\langle Y|\mathrm{e}^{\mathrm{i}\hat{Y}_C\hat{X}_A/2}\mathrm{e}^{-\mathrm{i}\hat{Y}_A\hat{X}_B/2}|\phi\rangle_C|X := 0\rangle_A|Y := 0\rangle_B. \tag{7.19}$$

Calculating this in the eigenbasis of $\hat{X}_B$ gives

$${}_B\langle x|\phi^{XY}\rangle_B \propto \mathrm{e}^{-\mathrm{i}Yx/2}{}_C\langle X + x|\phi\rangle_C. \tag{7.20}$$

**Exercise 7.9** *Show this, by first using the Baker–Campbell–Hausdorff theorem (A.118) to show that*

$$\mathrm{e}^{\mathrm{i}\hat{Y}_C\hat{X}_A/2}\mathrm{e}^{-\mathrm{i}\hat{Y}_A\hat{X}_B/2} = \mathrm{e}^{-\mathrm{i}\hat{Y}_A\hat{X}_B/2}\mathrm{e}^{\mathrm{i}\hat{Y}_C\hat{X}_A/2}\mathrm{e}^{\mathrm{i}\hat{Y}_C\hat{X}_B/2} \tag{7.21}$$

*and then recalling that $\mathrm{e}^{-\mathrm{i}\hat{Y}x/2}|X\rangle = |X + x\rangle$.*

Using the last part of this exercise a second time, we can write Eq. (7.20) in a basis-independent manner as

$$|\phi^{XY}\rangle_B \propto \mathrm{e}^{-\mathrm{i}Y\hat{X}_B/2}\mathrm{e}^{\mathrm{i}X\hat{Y}_B/2}|\phi\rangle_B. \tag{7.22}$$

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

Thus, up to two simple unitary transformations (displacements of the canonical variables), the conditional state of Bob's system is the same as the initial unknown client state. If Alice now sends the results of her measurements $(X, Y)$ to Bob, the two unitary transformations can be removed by local operations that correspond to a displacement in phase-space of $\hat{X}$ by $X$ and of $\hat{Y}$ by $Y$. Thus the initial state of the client has successfully been teleported to Bob. Note that in this case an infinite amount of information must be communicated by Alice, because $X$ and $Y$ are two real numbers. It is not difficult to verify that, just as in the qubit case, no information about $|\phi\rangle$ is contained in this communication.

This whole procedure is actually far simpler to see in the Heisenberg picture. Alice measures $\hat{X}_C - \hat{X}_A = \hat{X}$ and $\hat{Y}_C + \hat{Y}_A = \hat{Y}$. Note that here we are using the operators $\hat{X}$ and $\hat{Y}$ to denote the measurement results (see Section 1.3.2), but in the EPR state, $\hat{X}_A = \hat{X}_B$ and $\hat{Y}_A = -\hat{Y}_B$. Therefore Alice knows $\hat{X} = \hat{X}_C - \hat{X}_B$ and $\hat{Y} = \hat{Y}_C - \hat{Y}_B$. When she sends this information to Bob, Bob translates $\hat{X}_B \to \hat{X}'_B = \hat{X}_B + \hat{X} = \hat{X}_C$ and $\hat{Y}_B \to \hat{Y}'_B = \hat{Y}_B + \hat{Y} = \hat{Y}_C$. Now, since $\hat{X}_B$ and $\hat{Y}_B$ are by assumption a complete set of observables, all operators for Bob's system can be written as functions of $\hat{X}_B$ and $\hat{Y}_B$. Thus, since Bob's new observables are the same as the original observables for the client, it follows that all properties of Bob's system are the same as those of the client's original system. In other words, the client's system has been teleported to Bob.

**Exercise 7.10** *Perform a similar Heisenberg-picture analysis for the case of qubit teleportation.*
**Hint:** *You may find the operation* $\oplus$ *(see Section 1.3.3) useful.*

### *7.3.2 A more realistic protocol*

The EPR state (7.18) is not a physical state because it has infinite uncertainty in the local quadratures. Thus, if it were realized as a state for two harmonic oscillators, it would contain infinite energy. In a realistic protocol we must use a state with finite mean energy. In an optical setting, an approximation to the EPR state is the two-mode squeezed vacuum state [WM94a]. This is an entangled state for two modes of an optical field. It is defined in the number eigenstate basis for each oscillator as

$$|\psi\rangle_{AB} = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n |n\rangle_A \otimes |n\rangle_B, \tag{7.23}$$

where $\lambda \in [0, 1)$. This state is generated from the ground (vacuum) state $|0, 0\rangle$ by the unitary transformation

$$\hat{U}(r) = \mathrm{e}^{r(\hat{a}^\dagger\hat{b}^\dagger - \hat{a}\hat{b})}, \tag{7.24}$$

where $\lambda = \tanh r$ and $\hat{a}$ and $\hat{b}$ are the annihilation operators for Alice's and Bob's mode, respectively. Compare this with the unitary transformation defining the one-mode squeezed state (A.103).

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

The two-mode squeezed state (7.23) approximates the EPR state in the limit $\lambda \to 1$ ($r \to \infty$). This can be seen from the expression for $|\psi\rangle_{AB}$ in the basis of $\hat{X}_A$ and $\hat{X}_B$:

$$\psi(x_A, x_B) = {}_A\langle x_A|_B\langle x_B|\psi\rangle \tag{7.25}$$

$$= (2\pi)^{-1/2} \exp\left[-\frac{e^{2r}}{8}(x_A - x_B)^2 - \frac{e^{-2r}}{8}(x_A + x_B)^2\right]. \tag{7.26}$$

This should be compared with the corresponding equation for the EPR state (7.18),

$$\psi(x_A, x_B) \propto {}_A\langle x_A|_B\langle x_B|e^{-i\hat{Y}_A\hat{X}_B/2}|X := 0\rangle_A|Y := 0\rangle_B \tag{7.27}$$

$$\propto \delta(x_A - x_B). \tag{7.28}$$

From Eq. (7.26) it is not difficult to show that

$$\mathrm{Var}(\hat{X}_A - \hat{X}_B) = \mathrm{Var}(\hat{Y}_A + \hat{Y}_B) = 2e^{-2r}, \tag{7.29}$$

so that in the limit $r \to \infty$ the perfect EPR correlations are reproduced. This result can be more easily derived in a pseudo-Heisenberg picture.

**Exercise 7.11** *Consider the unitary operator $\hat{U}(r)$ as an evolution operator, with $r$ as a pseudo-time. Show that, in the pseudo-Heisenberg picture,*

$$\frac{\partial}{\partial r}(\hat{X}_A - \hat{X}_B) = -(\hat{X}_A - \hat{X}_B), \tag{7.30}$$

$$\frac{\partial}{\partial r}(\hat{Y}_A + \hat{Y}_B) = -(\hat{Y}_A + \hat{Y}_B). \tag{7.31}$$

*Hence, with $r = 0$ corresponding to the vacuum state $|0, 0\rangle$, show that, in the state (7.23), the correlations (7.29) result.*

If we use the finite resource (7.23), but follow the same teleportation protocol as for the ideal EPR state, the final state for Bob is still pure, and has the wavefunction (in the $X_B$ representation)

$$\phi_B^{(X,Y)}(x) = \int_{-\infty}^{\infty} dx'\, e^{-\frac{i}{2}x'Y}\psi(x, x')\phi_C(X + x'), \tag{7.32}$$

where $\phi_C(x)$ is the wavefunction for the client state and $\psi(x, x')$ is given by Eq. (7.26). Clearly in the limit $r \to \infty$ the teleportation works as before.

**Exercise 7.12** *Show that when the client state is an oscillator coherent state $|\alpha\rangle$, with $\alpha \in \mathbb{R}$, the teleported state at B is*

$$\phi_B^{(X,Y)}(x) = (2\pi)^{-1/4} \exp\left[-\frac{1}{4}(x - \tanh r(2\alpha - X))^2 - \frac{ixY}{2}\tanh r\right]. \tag{7.33}$$

For finite squeezing the state at B is not (even after the appropriate displacements in phase space) an exact replica of the client state. We are interested in the *fidelity*,

$$F = |\langle\phi|e^{\frac{i}{2}gY\hat{X}_B}e^{-\frac{i}{2}gX\hat{Y}_B}|\phi^{(X,Y)}\rangle|^2. \tag{7.34}$$

In the ideal teleportation $g = 1$, but here we allow for the *gain* $g$ to be non-unity. For finite squeezing, it is in fact usually optimal to choose $g \neq 1$.

**Exercise 7.13** *Show that for the client state a coherent state,* $|\alpha\rangle$*, the optimal choice of the gain is* $g = \tanh r$*, in which case the fidelity is given by*

$$F = \mathrm{e}^{-(1-g)^2|\alpha|^2}. \tag{7.35}$$

### *7.3.3 A criterion for demonstrating CV teleportation*

In a real experiment, the fidelity is going to be less than Eq. (7.35), because of imperfections in the preparation, measurement and control. Just as in the qubit case, we are interested in the following question: what is the minimum average fidelity (over some ensemble of client states) for the protocol to be considered quantum? In this case, we will consider the ensemble of all possible coherent states, because these are easy states to generate and it allows one to obtain an analytical result [BK98].

Suppose A and B share no entanglement at all. In that case the best option for A is to make a simultaneous measurement of $\hat{X}_C$ and $\hat{Y}_C$, obtaining the results $X$ and $Y$ [BK98, HWPC05]. These are then sent to B over a classical noiseless channel. Upon obtaining the results, B can displace an oscillator ground state to produce the coherent state $|\beta\rangle$, with $\beta = (X + \mathrm{i}Y)/2$. Of course, from run to run $\beta$ fluctuates, so the state that describes experiments over many runs is actually

$$\rho_B = \int \mathrm{d}^2\beta \, \wp(\beta)|\beta\rangle\langle\beta|. \tag{7.36}$$

As discussed in Example 4 in Section 1.2.5,[1] the probability distribution for $\beta$ when the client state is a coherent state, $|\alpha\rangle$ is

$$\wp(\beta) = \frac{1}{\pi}|\langle\alpha|\beta\rangle|^2 = \frac{1}{\pi}\mathrm{e}^{-|\alpha-\beta|^2}. \tag{7.37}$$

From this expression it is clear that the fidelity is the same for all coherent states under this classical protocol. Thus the average fidelity would then be given by

$$\bar{F} = \langle\alpha|\left[\int \mathrm{d}^2\beta \, \wp(\beta)|\beta\rangle\langle\beta|\right]|\alpha\rangle \tag{7.38}$$

$$= \int \frac{\mathrm{d}^2\beta}{\pi}\mathrm{e}^{-2|\alpha-\beta|^2}. \tag{7.39}$$

**Exercise 7.14** *Show that this evaluates to give* $\bar{F} = \frac{1}{2}$.
**Hint:** *For simplicity set* $\alpha = 0$ *and write* $\beta$ *in polar coordinates.*

Thus $\bar{F} = 0.5$ is the classical boundary for teleportation of a coherent state. To be useful, a quantum protocol would need to give an average fidelity greater than 0.5.

[1] Note the difference in definition of the quadratures by a factor of $\sqrt{2}$ between this chapter and the earlier chapter.

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

Strictly, it would be impossible to demonstrate an average fidelity greater than 0.5 for the coherent-state ensemble using the quantum teleportation protocol of Section 7.3.2. The reason for this is that for that protocol the teleportation fidelity depends upon the coherent amplitude $|\alpha|$ as given by Eq. (7.35). Because this decays exponentially with $|\alpha|^2$, if one averaged over the entire complex ($\alpha$) plane, one would obtain a fidelity close to zero. In practice (as discussed in the following subsection) only a small part of the complex plane near the vacuum state ($|\alpha| = 0$) was sampled. For a discussion of how decoherence of the entangled resource due to phase fluctuations will affect Eq. (7.35), see Ref. [MB99]. For a discussion of other criteria for characterizing CV quantum teleportation, see Refs. [RL98, GG01].

### 7.3.4 Experimental demonstration of CV teleportation

Quantum teleportation of optical coherent states was first demonstrated by the group of Kimble [FSB$^+$98]. In order to understand the experiment we must consider how some of the formal steps in the preceding analysis are done in the laboratory. The initial entangled resource $|\psi\rangle_{AB}$, shared by the sender Alice and the receiver Bob, is a two-mode optical squeezed state as discussed above. To a very good approximation such states are produced in the output of non-degenerate parametric down-conversion using a crystal with a second-order optical polarizability [WM94a].

The joint measurement of the quadrature operators $\hat{X}_C - \hat{X}_A$, $\hat{Y}_C + \hat{Y}_A$ on the client and sender mode can be thought of as coupling modes $A$ and $C$ using a unitary transformation followed by a measurement of the quadratures $\hat{X}_C$ and $\hat{Y}_A$. In quantum optics the coupling can be simply effected using a 50 : 50 beam-splitter. This is represented by the unitary transformation

$$U_{\rm bs}\begin{pmatrix}\hat{X}_A\\ \hat{Y}_A\\ \hat{X}_C\\ \hat{Y}_C\end{pmatrix}U_{\rm bs}^\dagger = \frac{1}{\sqrt{2}}\begin{pmatrix}\hat{X}_A - \hat{X}_C\\ \hat{Y}_A - \hat{Y}_C\\ \hat{X}_C + \hat{X}_A\\ \hat{Y}_C + \hat{Y}_A\end{pmatrix}. \tag{7.40}$$

From this it is clear that the post-beam-splitter quadrature measurements described above are equivalent to a pre-beam-splitter measurement of $\hat{X}_C - \hat{X}_A$ and $\hat{Y}_C + \hat{Y}_A$. These quadratures can be measured using homodyne detection, as discussed in Section 4.7.6. Such measurements of course absorb all of the light, leaving Alice with only classical information (the measurement results). In a realistic device, inefficiency and dark noise introduce extra noise into these measurements, as discussed in Section 4.8.

On receipt of Alice's measurement results, Bob must apply the appropriate unitary operator, a displacement, to complete the protocol. Displacements are easy to apply in quantum optics using another mode, prepared in a coherent state with large amplitude, and a beam-splitter with very high reflectivity for mode $B$. This is is discussed in Section 4.4.1. In the experiment the two modes used were actually at different frequencies, and the role

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

of the beam-splitter was played by an electro-optic modulator (EOM), which coherently mixes light at the two frequencies. The phase and amplitude of the modulation in the EOM were determined appropriately using Alice's results.

The experiment included an additional step to verify to what extent the state received by Bob faithfully reproduced the state of the client field. In this experiment the state of the client was a coherent state. In essence another party, Victor, is verifying the fidelity of the teleportation. This was done using homodyne detection to monitor the quadrature variances of the teleported state. Since the experiment dealt with broad-band fields the single-mode treatment we have discussed must be extended to deal with this situation. Without going into details, the basic technique is simple to understand. The noise power spectrum of the homodyne current obtained by Victor directly measures the quadrature operator variances as a function of frequency. (See Section 5.2.1.) Thus at any particular frequency Victor effectively selects a single mode.

The key feature that indicates success of the teleportation is a drop in the quadrature variance seen by Victor when Bob applies the appropriate displacement to his state. This is done by varying the gain $g$. If Bob does nothing to his state ($g = 0$), Victor gets one half of a two-mode squeezed state. Such a state has a quadrature noise level well above the vacuum level of the coherent state that the parties are trying to teleport. As Bob varies his gain, Victor will see the quadrature noise level fall until at precisely the right gain the teleportation is effected and the variance falls to the vacuum level of a coherent state (in the limit of high squeezing). In reality, the finite squeezing in the entangled state as well as extra sources of noise introduced in the detectors and control circuits will make the minimum higher than this. Furusawa *et al.* [FSB$^+$98] observed a minimum quadrature variance of $2.23 \pm 0.03$ times the vacuum level. This can be shown to correspond to a fidelity of $F = 0.58 \pm 0.02$. As discussed previously, this indicates that entanglement is an essential part of the protocol.

## 7.4 Errors and error correction

Information storage, communication and processing are physical processes and are subject to corruption by process noise. In the quantum case, this corruption can be identified with decoherence, as has been discussed in detail in Chapter 3. We say that noise or decoherence introduces *errors* into the information. A major part of the field of quantum information is methods to deal with such errors, most notably *quantum error correction*. In this section we introduce some of the basic concepts of quantum errors and error correction.

### *7.4.1 Types of quantum errors*

To begin, consider errors in a classical bit $B$. To introduce errors, we couple the bit to another system also described by a binary variable $\Xi$, which we will refer to as the environment.

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

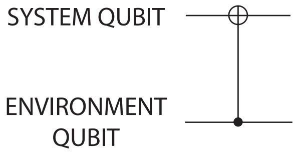

Fig. 7.2 Circuit diagram for a C-NOT interaction, which here represents the interaction of a two-state system with a two-state environment. In this case the value of the environment bit controls $(\cdot)$ a bit-flip error $(\oplus)$ on the target (the system bit). That is, if the environment bit has value 1, the value of the system bit changes, otherwise nothing happens. As discussed later, the same interaction or 'gate' can be applied to quantum bits, and this figure follows the conventions of Fig. 7.1.

Let the nature of the coupling be such as to transform the variables according to

$$B \to B \oplus \Xi, \tag{7.41}$$

$$\Xi \to \Xi. \tag{7.42}$$

The state of the environment is specified by the probability distribution

$$\wp(\xi := 1) = \mu = 1 - \wp(\xi := 0), \tag{7.43}$$

while the state of the system$\{\wp(b)\}$ is arbitrary. (See Section 1.1.2 for a review of notation.) This interaction or 'logic gate' is depicted in Fig. 7.2. Distinct physical systems (bits or qubits) are depicted as horizontal lines and interactions are depicted by vertical lines. In this case the interaction is referred to as a *controlled-NOT* or C-NOT gate, because the state of the lower system (environment) controls the state of the upper system according to the function defined in Eq. (7.41). The environment variable $\Xi$ is unchanged by the interaction; see Eq. (7.42).

This model becomes the *binary symmetric channel* of classical information theory [Ash90] when we regard $B$ as the input variable to a communication channel with output variable $B \oplus \Xi$. The received variable $B \oplus \Xi$ will reproduce the source variable $B$ iff $\Xi = 0$. Iff $\Xi = 1$, the received variable has undergone a 'bit-flip' error. This occurs with probability $\mu$, due to the noise or uncertainty in the environmental variable.

The same model can be used as a basis for defining errors in a qubit. The system variable $B$ is analogous to $(I + Z)/2$, where $Z$ is the system Pauli operator $Z_{\rm S}$. Likewise the environment variable $\Xi$ is analogous to $(I + Z)/2$, where here $Z$ is the environment Pauli operator $Z_{\rm E}$. The state of the environment is then taken as the mixed state

$$\rho_{\rm E} = (1 - \mu)|0\rangle\langle 0| + \mu|1\rangle\langle 1|. \tag{7.44}$$

A bit-flip error on the system is analagous to swapping the eigenstates of $Z$, which can be achieved by applying the system Pauli operator $X$. Thus we take the interaction to be specified by the unitary transformation

$$\hat{U} = X \otimes \frac{I - Z}{2} + I \otimes \frac{I + Z}{2} = \frac{1}{2}(XI - XZ + II + IZ). \tag{7.45}$$

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

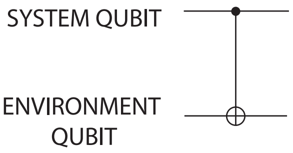

Fig. 7.3 Quantum circuit diagram for a C-NOT interaction that represents the interaction of a two-state system with a two-state environment. In this case the environment acts to produce (or not) a phase-flip error on the system qubit. Like all our quantum circuit diagrams, this figure follows the conventions of Fig. 7.1.

Here the order of operators is system then environment, and in the second expression we have dropped the tensor product, as discussed in Section 7.1.

**Exercise 7.15** *Show that the state (7.44) of the environment is left unchanged by this interaction, in analogy with Eq. (7.42).*

The system qubit after the interaction is given by

$$\rho'_{\mathrm{S}} = \mathrm{Tr}_{\mathrm{E}}\left[\hat{U}(\rho_{\mathrm{S}} \otimes \rho_{\mathrm{E}})\hat{U}^{\dagger}\right] \tag{7.46}$$

$$= \mu X \rho_{\mathrm{S}} X + (1-\mu)\rho_{\mathrm{S}}, \tag{7.47}$$

where $\rho_{\mathrm{S}}$ is the state of the system qubit before the interaction.

**Exercise 7.16** *Show this, and show that it also holds if the environment is prepared in the pure state* $\sqrt{1-\mu}\,|0\rangle + \sqrt{\mu}\,|1\rangle$.

In this form the interpretation of the noisy channel as an error process is quite clear: $\rho'_{\mathrm{S}}$ is the ensemble made up of a fraction $\mu$ of qubits that have suffered a bit-flip error and a fraction $1-\mu$ that have not.

**Exercise 7.17** *Show that the unitary operator in Eq. (7.45) can be generated by the system–environment interaction Hamiltonian*

$$\hat{H} = \frac{\kappa}{4}(I - X)(I + Z) \tag{7.48}$$

*for times* $\kappa t = \pi$.

From the discussion so far, it might seem that there is no distinction between errors for classical bits and qubits. This is certainly not the case. A new feature arises in the quantum case on considering the example depicted in Fig. 7.3. This is the same as the previous example in Fig. 7.2, except that the direction of the C-NOT gate has been reversed. In a classical description this would do nothing at all to the system bit. The quantum case is different. The interaction is now described by the unitary operator

$$\hat{U} = \frac{1}{2}(IX - ZX + II + ZI). \tag{7.49}$$

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

As in the previous example, we can take the initial state of the environment to be such that it is left unchanged by the interaction,

$$\rho_{\rm E} = (1-\mu)|+\rangle\langle+| + \mu|-\rangle\langle-|, \tag{7.50}$$

where $X|\pm\rangle = \pm 1|\pm\rangle$. Equivalently (for what follows) we could take it to be the superposition $\sqrt{1-\mu}\,|+\rangle + \sqrt{\mu}\,|-\rangle$.

The reduced state of the system at the output is now seen to be

$$\rho'_{\rm S} = \mu Z\rho_{\rm S}Z + (1-\mu)\rho_{\rm S}. \tag{7.51}$$

We can interpret this as describing an ensemble in which a fraction $1-\mu$ of systems remains unchanged while a fraction $\mu$ suffers the action of a $Z$-error. We will call this a phase-flip error since it changes the relative phase between matrix elements in the logical basis. In the logical basis the transformation is

$$\rho'_{\rm S} = \begin{pmatrix} \rho_{00} & (1-2\mu)\rho_{01} \\ (1-2\mu)\rho_{10} & \rho_{11} \end{pmatrix}, \tag{7.52}$$

where $\rho_{kl} = \langle k|\rho_{\rm S}|l\rangle$. The diagonal matrix elements in the logical basis are not changed by this transformation. This is a reflection of the classical result that the state of the system bit is unchanged. However, clearly the state is changed, and, for $0.5 < \mu < 1$, decoherence occurs: the magnitudes of off-diagonal matrix elements in the logical basis are decreased between input and output. Indeed, when $\mu = 0.5$, the state in the logical basis is completely decohered, since the off-diagonal matrix elements are zero at the output.

Having seen bit-flip errors, and phase-flip errors, it is not too surprising to learn that we can define a final class of qubit error by a channel that transforms the input system qubit state according to

$$\rho'_{\rm S} = \mu Y\rho_{\rm S}Y + (1-\mu)\rho_{\rm S}, \tag{7.53}$$

where $Y = -{\rm i}XZ$ (here this product is an ordinary matrix product, not a tensor product). This error is a simultaneous bit-flip and phase-flip error. All errors can be regarded as some combination of these elementary errors. In reality, of course, a given decoherence process will not neatly fall into these categories of bit-flip or phase-flip errors. However, the theory of quantum error correction shows that if we can correct for these elementary types of errors then we can correct for an arbitrary single-qubit decoherence process [NC00].

### 7.4.2 *Quantum error correction*

The basic idea behind quantum error correction (QEC) is to encode the state of a logical qubit into more than one physical qubit. This can be understood most easily in the case of a single type of error (e.g. bit-flip errors). In that case, an encoding system that is similar to the simple classical redundancy encoding may be used. In the classical case, we simply copy the information ($X = 0$ or 1) in one bit into (say) two others. Then, after a short time, a bit-flip error may have occurred on one bit, but it is very unlikely to have occurred

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

Table 7.1. *The three-qubit bit-flip code*

| $ZZI$ | $IZZ$ | Error | Correcting unitary |
|---|---|---|---|
| $+1$ | $+1$ | None | None |
| $-1$ | $+1$ | On qubit 1 | $XII$ |
| $+1$ | $-1$ | On qubit 3 | $IIX$ |
| $-1$ | $-1$ | On qubit 2 | $IXI$ |

on two and even less likely to have occurred on all three. (A crucial assumption here is the independence of errors across the different bits. Some form of this assumption is also necessary for the quantum case.) The occurrence of an error can be detected by measuring the parity of the bit values, that is, whether they are all the same or not. If one is different, then a majority vote across the bits as to the value of $X$ is very likely to equal the original value, even if an error has occurred on one bit. This estimate for $X$ can then be used to change the value of the minority bit. This is the process of error correction.

These ideas can be translated into the quantum case as follows. We encode the qubit state in a two-dimensional subspace of the multi-qubit tensor-product space, known as the code space. The basis states for the code space, known as code words, are entangled states in general. For a three-qubit code to protect against bit-flip errors we can choose the code words to be simply

$$|0\rangle_L = |000\rangle, \qquad |1\rangle_L = |111\rangle. \tag{7.54}$$

An arbitrary pure state of the logical qubit then has the form $|\psi\rangle_L = \alpha|000\rangle + \beta|111\rangle$.

Suppose one of the physical qubits undergoes a bit-flip. It is easy to see that, no matter which qubit flips, the error state is always orthogonal to the code space and simultaneously orthogonal to the other two error states.

**Exercise 7.18** *Show this.*

This is the crucial condition for the error to be detectable and correctable, because it makes it possible, in principle, to detect which *physical* qubit has flipped, without learning anything about the *logical* qubit, and to rotate the error state back to the code space. Unlike in the classical case, we cannot simply read out the qubits in the logical basis, because that would destroy the superposition. Rather, to detect whether and where the error occurred, we must measure the two commuting operators $ZZI$ and $IZZ$. (We could also measure the third such operator, $ZIZ$, but that would be redundant.) The result of this measurement is the *error syndrome*. Clearly there are two possible outcomes for each operator ($\pm1$) to give four error syndromes. These are summarized in Table 7.1.

The above encoding is an example of a *stabilizer code* [Got96]. In general this is defined as follows. First, we define the Pauli group for $n$ qubits as

$$\mathfrak{P}_n = \{\pm1, \pm\mathrm{i}\} \otimes \{I, X, Y, Z\}^{\otimes n}. \tag{7.55}$$

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

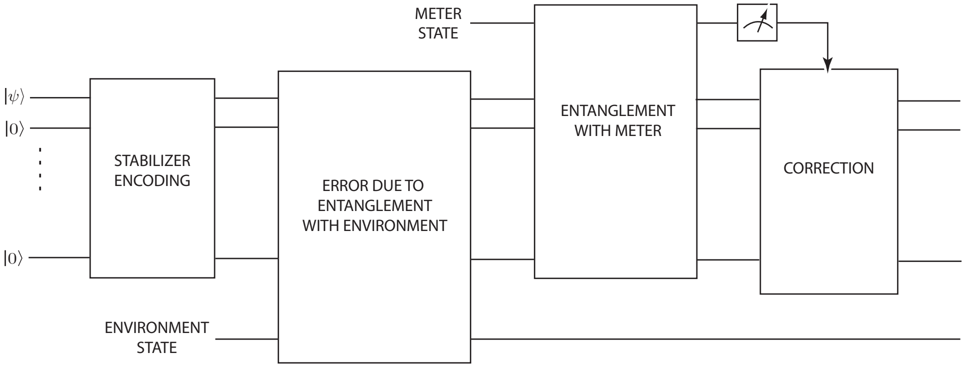

Fig. 7.4 The conventional error-correction protocol using the stabilizer formalism. After the state has been encoded, an error occurs through coupling with the environment. To correct this error, the encoded state is entangled with a meter in order to measure the stabilizer generators, and then feedback is applied on the basis of those measurements. Figure 1 adapted with permission from C. Ahn *et al.*, *Phys. Rev.* A **67**, 052310, (2003). Copyrighted by the American Physical Society.

That is, any member may be denoted as a concatenation of letters (such as $ZZI$ above for $n = 3$) times a phase factor of $\pm 1$ or $\pm$i. Note that this is a discrete group (here a set of operators closed under mutiplication), not a Lie group – see Box 6.2. It can be shown that there exist subgroups of $2^{n-k}$ commuting Pauli operators $\mathfrak{S} \in \mathfrak{P}_n$ for all $n \geq k \geq 0$. Say that $-I$ is not an element of $\mathfrak{S}$ and that $k \geq 1$. Then it can be shown that $\mathfrak{S}$ defines the *stabilizer* of a nontrivial quantum code. The code space $C(\mathfrak{S})$ is the simultaneous $+1$ eigenspace of all the operators in $\mathfrak{S}$. Then the subspace stabilized is nontrivial, and the dimension of $C(\mathfrak{S})$ is $2^k$. Hence this system can encode $k$ logical qubits in $n$ physical qubits. In the above example, we have $n = 3$ and $k = 1$.

The generators of the stabilizer group are defined to be a subset of this group such that any element of the stabilizer can be described as a product of generators. Note that this terminology differs from that used to define generators for Lie groups – see Box 6.2. It can be shown that $n - k$ generators suffice to describe the stabilizer group $\mathfrak{S}$. In the above example, we can take the generators of $\mathfrak{S}$ to be $ZZI$ and $IZZ$, for example. As this example suggests, the error-correction process consists of measuring the stabilizer. This projection discretizes whatever error has occurred into one of $2^{n-k}$ error syndromes labelled by the $2^{n-k}$ possible outcomes of the stabilizer generator measurements. This information is then used to apply a unitary recovery operator that returns the state to the code space. A diagram of how such a protocol would be implemented in a physical system is given in Fig. 7.4.

To encode a single ($k = 1$) logical qubit against bit-flip errors, only three ($n = 3$) physical qubits are required. However, to encode against arbitrary errors, including phase-flips, a larger code must be used. The smallest *universal* encoding uses code words of length $n = 5$ [LMPZ96]. Since this has $k = 1$, the stabilizer group has four generators, which can be chosen to be

$$XZZXI,\ IXZZX,\ XIXZZ,\ ZXIXZ. \tag{7.56}$$

However, unlike the above example, this is not based on the usual classical codes (called linear codes), which makes it hard to generalize. The smallest universal encoding based on combining linear codes is the $n = 7$ Steane code [Ste96].

### 7.4.3 Detected errors

It might be thought that if one had direct knowledge of whether an error occurred, and precisely what error it was, then error correction would be trivial. Certainly this is the case classically: if one knew that a bit had flipped then one could just flip it back; no encoding is necessary. The same holds for the reversible (unitary) errors we have been considering, such as bit-flip ($X$), phase-flip ($Z$) or both ($Y$). For example, if one knew that a $Z$-error had occurred on a particular qubit, one would simply act on that qubit with the unitary operator $Z$. This would completely undo the effect of the error since $Z^2 = I$; again, no encoding is necessary. From the model in Section 7.4.1, one can discover whether or not a $Z$-error has occurred simply by measuring the state of the environment in the logical basis.

However, we know from earlier chapters to be wary of interpreting the ensemble resulting from the decoherence process (7.47) in only one way. If we measure the environment in the $|\pm\rangle$ basis then we do indeed find a $Z$-error with probability $\mu$, but if we measure the environment in a different basis (which may be forced upon us by its physical context, as described in Chapter 3) then a different sort of error will be found. In particular, for the case $\mu = 1/2$ and the environment initially in a superposition state, we reproduce exactly the situation of Section 1.2.6. That is, if we measure the environment in the logical basis (which is conjugate to the $|\pm\rangle$ basis), then we discover not whether or not the qubit underwent a phase-flip, but rather which logical state the qubit is in.

**Exercise 7.19** *Verify this.*

Classically such a measurement does no harm of course, but in the quantum case it changes the system state irreversibly. That is, there is no way to go back to the (unknown) pre-measurement state of the qubit. Moreover, there are some sorts of errors, which we will consider in Section 7.4.4, that are inherently irreversible. That is, there is no way to detect the error without obtaining information about the system and hence collapsing its state.

These considerations show that the effect of detected errors is nontrivial in the quantum case. Of course, we can correct any errors simply by ignoring the result of the measurement of the environment and using a conventional quantum error correcting protocol, as explained in Section 7.4.2. However, we can do better if we use quantum encoding *and* make use of the measurement results. That is, we can do the encoding using fewer physical qubits. The general idea is illustrated in Fig. 7.5. A simple example is $Z$-measurement as discussed above. Since this is equivalent to phase-flip errors, it can be encoded against using the three-qubit code of Eq. (7.54). However, if we record the results of the $Z$-measurements, then we can correct these errors using just a two-qubit code, as we now show. This is not just a hypothetical case; accidental $Z$-measurements are intrinsic to various schemes for linear optical quantum computing [KLM01].

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

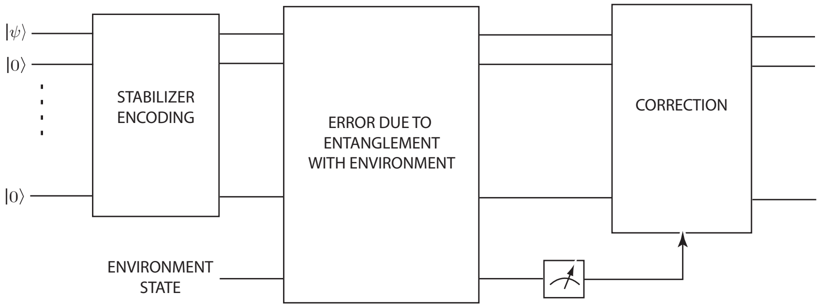

Fig. 7.5 A modified error-correction protocol using the stabilizer formalism but taking advantage of the information obtained from measuring the environment. That is, in contrast to Fig. 7.4, the error and measurement steps are the same. The correction is, of course, different from Fig. 7.4 also. Figure 1 adapted with permission from C. Ahn *et al.*, *Phys. Rev.* A **67**, 052310, (2003). Copyrighted by the American Physical Society.

We can still use the stabilizer formalism introduced above to deal with the case of detected errors. For $Z$-measurements, we have $n = 2$ and $k = 1$, so there is a single stabilizer generator, which can be chosen to be $XX$. This gives a code space spanned by the code words

$$\sqrt{2}|0\rangle_L = |00\rangle + |11\rangle, \tag{7.57}$$

$$\sqrt{2}|1\rangle_L = |01\rangle + |10\rangle. \tag{7.58}$$

**Exercise 7.20** *Show that in this case* $\mathfrak{S} = \{XX, II\}$ *and verify that the code words are* $+1$ *eigenstates of both of the operators in* $\mathfrak{S}$.

Suppose now that we have an arbitrary qubit state, $|\psi\rangle = \alpha|0\rangle_L + \beta|1\rangle_L$. If the first qubit is accidentally measured in the logical basis, with result 0, the conditional state is $\alpha|00\rangle + \beta|01\rangle = |0\rangle(\alpha|0\rangle + \beta|1\rangle)$. Thus the logical qubit state is still preserved in the state of the second qubit.

**Exercise 7.21** *Show that the state with this error is rotated back to the correct encoded state using the operator*

$$\hat{U} = \frac{1}{\sqrt{2}}(XX + ZI). \tag{7.59}$$

In general, if an accidental measurement of qubit 1 or 2 gives result $x$, the encoded state is recovered if we apply the respective corrections

$$\hat{U}_1^{(x)} = \frac{1}{\sqrt{2}}(XX + (-1)^x ZI), \tag{7.60}$$

$$\hat{U}_2^{(x)} = \frac{1}{\sqrt{2}}(XX + (-1)^x IZ). \tag{7.61}$$

### 7.4.4 Dynamical decoherence

The discussion so far has been largely unconcerned with dynamics. QEC arose in connection with quantum computing where the dynamics is reduced to a set of unitary operations (gates), applied at discrete times, with no dynamics in between. In the early studies of error correction, errors were modelled as occurring, probabilistically, at discrete times. The detection of a syndrome and subsequent correction were also applied, like gates, at discrete times. That is, the measurement of the error syndrome was assumed to be ideal and instantaneous. This is not a very realistic scenario. Errors are often due to continuous interactions with other systems and thus are dynamical stochastic processes occurring continously in time. Likewise the measurement of an error syndrome must take some time and is a dynamical process that may have extra noise. Finally, one might expect that an error-correction operation may itself take some time to implement.

We have discussed in Chapter 3 how decoherence can be described as a dynamical process, the simplest model being a Markov master equation. For any particular physical implementation of quantum computation a detailed experimental study of the likely sources of decoherence needs to be made and an appropriate model defined. This is easier for some schemes than for others. Ion-trap implementations have well-characterized decoherence processes [Ste07], as do quantum-optical schemes [LWP$^+$05], while for many solid-state schemes these studies have only just begun [SAB$^+$06, TMB$^+$06]. In this chapter we will consider a simple model of continuous errors that leads directly to a Markov master equation.

Consider the case of phase-flip errors. Let us suppose that, at Poisson-distributed times, the state of the system is transformed according to $\rho \to Z\rho Z$. That is, the rate of the process is a constant, say $\gamma$, that is independent of the state of the system. Then, in an infinitesimal interval of time $\mathrm{d}t$, the change in the state is given by the mixture of states that have been so transformed and those that have not:

$$\rho(t + \mathrm{d}t) = \gamma\, \mathrm{d}t\, Z\rho(t)Z + (1 - \gamma\, \mathrm{d}t)\rho(t), \tag{7.62}$$

from which it follows that

$$\dot{\rho} = \gamma(Z\rho Z - \rho) = \gamma\mathcal{D}[Z]\rho. \tag{7.63}$$

**Exercise 7.22** *Show that this equation also describes monitoring of whether the system is in logical state* 0, *for example.*
**Hint:** *Note that* $Z + I = 2\pi_0$, *with* $\pi_0 = |0\rangle\langle 0|$, *and show that Eq. (7.63) can be unravelled using the measurement operators*

$$\hat{M}_1 = \sqrt{4\gamma\, \mathrm{d}t}\; \pi_0, \tag{7.64}$$

$$\hat{M}_0 = 1 - 2\gamma\, \mathrm{d}t\, \pi_0. \tag{7.65}$$

Another example of continuously occurring errors – which *cannot* be thought of as Poisson-distributed unitary errors – is spontaneous emission. Consider a register of $n$ qubits, each coupled to an independent bath. The measurement operator for a spontaneous

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

emission event on the $j$th qubit, in an infinitesimal time interval, takes the form

$$\hat{M}_1^j(\mathrm{d}t) = \sqrt{\kappa_j\,\mathrm{d}t}\,(X_j - \mathrm{i}Y_j)/2 \equiv \sqrt{\kappa_j\,\mathrm{d}t}\,L_j, \tag{7.66}$$

where $\kappa_j$ is the decay rate for the $j$th qubit, and we have defined the *lowering operator* $L_j = |1\rangle_j\langle 0|_j$. The corresponding no-jump measurement operator is

$$\hat{M}_0(\mathrm{d}t) = 1 - \sum_j(\kappa_j/2)L_j^\dagger L_j\,\mathrm{d}t - \mathrm{i}\hat{H}\,\mathrm{d}t, \tag{7.67}$$

where, as in Section 4.2, we have allowed for the possibility of some additional Hamiltonian dynamics. The master equation for the $n$-qubit system is thus

$$\dot{\rho} = \sum_j \kappa_j\mathcal{D}[L_j]\rho - \mathrm{i}[\hat{H}, \rho]. \tag{7.68}$$

**Exercise 7.23** *Show that, for* $\hat{H} = 0$, *the coherence of the $j$th qubit, as measured by* $\langle X_j(t)\rangle$ *or* $\langle Y_j(t)\rangle$, *decays exponentially with lifetime* $T_2 = 2/\kappa_j$, *while the probability of its occupying logical state* $|0\rangle$, *as measured by* $\left\langle Z_j(t) + 1\right\rangle/2$, *decays exponentially with lifetime* $T_1 = 1/\kappa_j$. *Here the lifetime is defined as the time for the exponential to decay to* $\mathrm{e}^{-1}$.

In the following section we will show that the techniques of correcting detected errors introduced in Section 7.4.3 can be adapted to deal with continuous detections, whether non-demolition, as in Eq. (7.64), or demolition, as in Eq. (7.66).

## 7.5 Feedback to correct continuously detected errors

In this section we consider monitored errors, that is, continuously detected errors. We assume initially that there is only one error channel for each physical qubit. We show that, for any error channel and any method of detection (as long as it is efficient), it is possible to correct for these errors using an encoding that uses only one excess qubit. That is, using $n$ physical qubits it is possible to encode $n-1$ logical qubits, using the stabilizer formalism. This section is based upon Ref. [AWM03].

### *7.5.1 Feedback to correct spontaneous emission jumps*

Rather than considering encoding and error correction for an arbitrary model of continuously detected errors, we begin with a specific model and build up its generality in stages. The simple model we begin with is for encoding one logical qubit against detected spontaneous emission events. This was considered first by Mabuchi and Zoller [MZ96], for a general physical system, and subsequently by several other authors in the context of encoding in several physical qubits [PVK97, ABC$^+$01, ABC$^+$03]. The model we present here gives the most efficient encoding, because we allow a constant Hamiltonian in addition to the feedback Hamiltonian. Specifically, we show that by using a simple two-qubit code

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

we can protect a one-qubit code space perfectly, provided that the spontaneously emitting qubit is known and a correcting unitary is applied instantaneously.

The code words of the code were previously introduced in Eqs. (7.57) and (7.58). If the emission is detected, such that the qubit $j$ from which it originated is known, it is possible to correct back to the code space without knowing the state. This is because the code and error fulfil the necessary and sufficient conditions for appropriate recovery operations [KL97]:

$$\langle\mu|\hat{E}^\dagger\hat{E}|\nu\rangle = \Lambda_E\delta_{\mu\nu}. \tag{7.69}$$

Here $\hat{E}$ is the operator for the measurement (error) that has occurred and $\Lambda_E$ is a constant. The states $|\mu\rangle$ form an orthonormal basis for the code space (they could be the logical states, such as $|0\rangle_L$ and $|1\rangle_L$ in the case of a single logical qubit). These conditions differ from the usual condition only by taking into account that we *know* a particular error $\hat{E} = L_j$ has occurred, rather than having to sum over all possible errors.

**Exercise 7.24** *Convince yourself that error recovery is possible if and only if Eq. (7.69) holds for all measurement (error) operators $\hat{E}$ to which the system is subject.*

More explicitly, if a spontaneous emission on the first qubit occurs, $|0\rangle_L \to |01\rangle$ and $|1\rangle_L \to |00\rangle$. Since these are orthogonal states, this fulfills the condition given in (7.69), so a unitary exists that will correct this spontaneous emission error. One choice for the correcting unitary is

$$\hat{U}_1 = (XI + ZX)/\sqrt{2}, \tag{7.70}$$

$$\hat{U}_2 = (IX + XZ)/\sqrt{2}. \tag{7.71}$$

**Exercise 7.25** *Verify that these are unitary operators and that they correct the errors as stated.*

As discussed above, in this jump process the evolution between jumps is non-unitary, and so also represents an error. For this two-qubit system the no-jump infinitesimal measurement operator Eq. (7.67) is

$$\hat{M}_0(\mathrm{d}t) = 1 - \frac{\kappa_1}{2}L_1^\dagger L_1\,\mathrm{d}t - \frac{\kappa_2}{2}L_2^\dagger L_2\,\mathrm{d}t - \mathrm{i}\hat{H}\,\mathrm{d}t \tag{7.72}$$

$$= II - \mathrm{d}t[(\kappa_1+\kappa_2)II + \kappa_1 ZI + \kappa_2 IZ + \mathrm{i}\hat{H}]. \tag{7.73}$$

The non-unitary part of this evolution can be corrected by assuming a driving Hamiltonian of the form

$$\hat{H} = -(\kappa_1 YX + \kappa_2 XY). \tag{7.74}$$

This result can easily be seen by plugging (7.74) into (7.73) with a suitable rearrangement of terms:

$$\hat{M}_0(\mathrm{d}t) = II[1-(\kappa_1+\kappa_2)\mathrm{d}t] - \kappa_1\,\mathrm{d}t\,ZI(II-XX) - \kappa_2\,\mathrm{d}t\,IZ(II-XX). \tag{7.75}$$

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

**Exercise 7.26** *Verify this.*

Since $II - XX$ acts to annihilate the code space, $\hat{M}_0$ acts trivially on the code space.

Including the unitary feedback and the driving Hamiltonian, we then have the following master equation for the evolution of the system:

$$d\rho = \hat{M}_0(dt)\rho\hat{M}_0^\dagger(dt) - \rho + dt\sum_{j=1}^{2}\kappa_j\hat{U}_jL_j\rho L_j^\dagger\hat{U}_j^\dagger. \tag{7.76}$$

On writing this in the Lindblad form, we have

$$\dot{\rho} = \sum_{j=1}^{2}\kappa_j\mathcal{D}[\hat{U}_jL_j]\rho + i[\kappa_1YX + \kappa_2XY, \rho]. \tag{7.77}$$

From Section 5.4.2, the unitary feedback can be achieved by a feedback Hamiltonian of the form

$$\hat{H}_{fb} = I_1(t)\hat{V}_1 + I_2(t)\hat{V}_2. \tag{7.78}$$

Here $I_j(t) = dN_j(t)/dt$ is the observed photocurrent from the emissions by the $j$th qubit, while $\hat{V}_j$ is an Hermitian operator such that $\exp(-i\hat{V}_j) = \hat{U}_j$.

**Exercise 7.27** *Show that choosing* $\hat{V}_j = (\pi/2)\hat{U}_j$ *works.*
**Hint:** *Show that* $\hat{U}_j^2 = I$, *like a Pauli operator.*

This code is optimal in the sense that it uses the smallest possible number of qubits required to perform the task of correcting a spontaneous emission error, since we know that the information stored in one unencoded qubit is destroyed by spontaneous emission.

### *7.5.2 Feedback to correct spontaneous-emission diffusion*

So far we have considered only one unravelling of spontaneous emission, by direct detection giving rise to quantum jumps. However, as emphasized in Chapter 4, other unravellings are possible, giving rise to quantum diffusion for example. In this subsection we consider homodyne detection (which may be useful experimentally because it typically has a higher efficiency than direct detection) and show that the same encoding allows quantum diffusion also to be corrected by feedback.

As shown in Section 4.4, homodyne detection of radiative emission of the two qubits gives rise to currents with white noise,

$$J_j(t)dt = \kappa_j\langle e^{-i\phi_j}L_j + e^{i\phi_j}L_j^\dagger\rangle dt + \sqrt{\kappa_j}\,dW_j(t). \tag{7.79}$$

Choosing the $Y$-quadratures ($\phi_j = \pi/2\ \forall j$) for definiteness, the corresponding conditional evolution of the system is

$$d\rho_{\bar{J}}(t) = -i[\hat{H}, \rho_{\bar{J}}]dt + \sum_{j=1}^{2}\kappa_j\mathcal{D}[L_j]\rho_{\bar{J}}\,dt + \sum_{j=1}^{2}\sqrt{\kappa_j}\mathcal{H}[-iL_j]\rho_{\bar{J}}\,dW_j(t). \tag{7.80}$$

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

We can now apply the homodyne mediated feedback scheme introduced in Section 5.5. With the feedback Hamiltonian

$$\hat{H}_{\rm fb} = \sqrt{\kappa_1}\hat{F}_1 J_1(t) + \sqrt{\kappa_2}\hat{F}_2 J_2(t), \tag{7.81}$$

the resulting Markovian master equation is

$$\dot{\rho} = -{\rm i}[\hat{H},\rho] - {\rm i}\sum_{j=1}^{2}\kappa_j\Big\{[{\rm i}(L_j^\dagger \hat{F}_j - \hat{F}_j L_j)/2, \rho] + \mathcal{D}[{\rm i}L_j - {\rm i}\hat{F}_j]\rho\Big\}. \tag{7.82}$$

This allows us to use the same code words, and Eqs. (7.70) and (7.71) suggest using the following feedback operators:

$$\begin{aligned}\hat{F}_1 &= XI + ZX,\\ \hat{F}_2 &= IX + XZ.\end{aligned} \tag{7.83}$$

Using also the same driving Hamiltonian (7.74) as in the jump case, the resulting master equation is

$$\dot{\rho} = \kappa_1\mathcal{D}[YI - {\rm i}ZX]\rho + \kappa_2\mathcal{D}[IY - {\rm i}XZ]\rho. \tag{7.84}$$

**Exercise 7.28** *Verify this, and show that it preserves the above code space.*
**Hint:** *First show that* $YI - {\rm i}ZX = YI(II - XX)$.

### *7.5.3 Generalization to spontaneous emission of n qubits*

We will now demonstrate a simple $n$-qubit code that allows correction of spontaneous-emission errors, while encoding $n-1$ qubits. Both of the above calculations (jump and diffusion) generalize. The master equation is the same as (7.68), and the index $j$ runs from 1 to $n$. Again we need only a single stabilizer generator, namely $X^{\otimes n}$. The number of code words is thus $2^{n-1}$, enabling $n-1$ logical qubits to be encoded. Since it uses only one physical qubit in excess of the number of logical qubits, this is again obviously an optimal code.

First, we consider the jump case. As previously, a spontaneous-emission jump fulfils the error-correction condition (7.69) (this will be shown in an even more general case in the following subsection). Therefore there exists a unitary that will correct for the spontaneous-emission jump. Additionally, it is easy to see by analogy with (7.75) that

$$\hat{H} = \kappa_j \sum_j X^{\otimes j-1} Y X^{\otimes n-j} \tag{7.85}$$

protects against the nontrivial no-emission evolution. Therefore the code space is protected.

Next, for a diffusive unravelling, we again choose homodyne measurement of the $Y$-quadrature. The same driving Hamiltonian (7.85) is again required, and the feedback operators generalize to

$$\hat{F}_j = I^{\otimes j-1} X I^{\otimes n-j} + X^{\otimes j-1} Z X^{\otimes n-j}. \tag{7.86}$$

The master equation becomes

$$\dot{\rho} = \sum_j \kappa_j \mathcal{D}[I^{\otimes j-1} Y I^{\otimes n-j}(I^{\otimes n} - X^{\otimes n})], \tag{7.87}$$

which manifestly has no effect on states in the code space.

### 7.5.4 Generalization to arbitrary local measurements on n qubits

In this section, we generalize the above theory to $n$ qubits with arbitrary local (that is, single-qubit) measurements. We find the condition that the stabilizers of the code space must satisfy and show that it is always possible to find an optimal code space (that is, one with a single stabilizer group generator). We give the explicit feedback protocol for a family of unravellings parameterized by a complex number $\gamma$, as introduced in Section 4.4. A simple jump unravelling has $\gamma = 0$, while the diffusive unravelling requires $|\gamma| \to \infty$, with the measured quadrature defined by $\phi = \arg(\gamma)$.

Consider a Hilbert space of $n$ qubits obeying (7.68), but with the lowering operators $L_j$ replaced by arbitrary single-qubit operators $\hat{c}_j$ and with $\kappa_j \equiv 1$ (which is always possible since these rates can be absorbed into the definitions of $\hat{c}_j$). Let us consider a single jump operator $\hat{c}$ acting on a single qubit. We may then write $\hat{c}$ in terms of traceless Hermitian operators $\hat{A}$ and $\hat{B}$ as

$$e^{-i\phi}\hat{c} = \chi I + \hat{A} + i\hat{B} \equiv \chi I + \vec{a}\cdot\vec{\sigma} + i\vec{b}\cdot\vec{\sigma}, \tag{7.88}$$

where $\chi$ is a complex number, $\vec{a}$ and $\vec{b}$ are real vectors, and $\vec{\sigma} = (X, Y, Z)^\top$.

We now use the standard condition (7.69), where here we take $\hat{E} = \hat{c} + \gamma$ (see Section 4.4). Henceforth, $\gamma$ is to be understood as real and positive, since the relevant phase $\phi$ has been taken into account in the definition (7.88). From Eq. (7.69), we need to consider

$$\begin{aligned} \hat{E}^\dagger\hat{E} &= (|\chi+\gamma|^2 + \vec{a}^2 + \vec{b}^2)I + \mathrm{Re}(\chi+\gamma)\hat{A} + \mathrm{Im}(\chi+\gamma)^* i\hat{B} + (\vec{a}\times\vec{b})\cdot\vec{\sigma} \\ &\equiv (|\chi+\gamma|^2 + \vec{a}^2 + \vec{b}^2)I + \hat{D}, \end{aligned} \tag{7.89}$$

where $\hat{D}$ is Hermitian and traceless.

Now the sufficient condition for error correction for a stabilizer code is that the stabilizer should anticommute with the traceless part of $E^\dagger E$ [Got96]. This condition becomes explicitly

$$0 = \{\hat{S}, \hat{D}\}. \tag{7.90}$$

As long as this is satisfied, there is some feedback unitary $e^{-iV}$ that will correct the error.

As usual, even when the error with measurement operator $\sqrt{dt}\,\hat{E}$ does not occur, there is still non-unitary evolution. As shown in Section 4.4, it is described by the measurement operator

$$\hat{M}_0 = 1 - \hat{E}^\dagger \hat{E}\,\mathrm{d}t - \frac{|\gamma|}{2}(\mathrm{e}^{-\mathrm{i}\phi}\hat{c} - \mathrm{e}^{\mathrm{i}\phi}\hat{c}^\dagger)\mathrm{d}t - \mathrm{i}\hat{H}\,\mathrm{d}t. \tag{7.91}$$

Now we choose the driving Hamiltonian

$$\hat{H} = \mathrm{i}\hat{D}\hat{S} + \frac{\mathrm{i}|\gamma|}{2}(\mathrm{e}^{-\mathrm{i}\phi}\hat{c} - \mathrm{e}^{\mathrm{i}\phi}\hat{c}^\dagger). \tag{7.92}$$

This is an Hermitian operator because of (7.90).

**Exercise 7.29** *Show that, with this choice, $\hat{M}_0$ is proportional to the identity plus a term proportional to $\hat{D}(1 - \hat{S})$, which annihilates the code space.*

Thus, for a state initially in the code space, the condition (7.90) suffices for correction of both the jump and the no-jump evolution.

We now have to show that a single $\hat{S}$ exists for all qubits, even with different operators $\hat{c}_j$. Since $\hat{D}_j$ (the operator associated with $\hat{c}_j$ as defined in (7.89)) is traceless, it is always possible to find some other Hermitian traceless one-qubit operator $\hat{s}_j$, such that $\{\hat{s}_j, \hat{D}_j\} = 0$ and $\hat{s}_j^2 = I$. Then we may choose the single stabilizer generator

$$\hat{S} = \hat{s}_1 \otimes \cdots \otimes \hat{s}_n \tag{7.93}$$

so that the stabilizer group[2] is $\{\hat{1}, \hat{S}\}$. Having chosen $\hat{S}$, choosing $\hat{H}$ as

$$\hat{H} = \sum_j \mathrm{i}\hat{D}_j\hat{S} + \frac{\mathrm{i}|\gamma_j|}{2}(\mathrm{e}^{-\mathrm{i}\phi_j}\hat{c}_j - \mathrm{e}^{\mathrm{i}\phi_j}\hat{c}_j^\dagger) \tag{7.94}$$

will, by our analysis above, provide a total evolution that protects the code space, and the errors will be correctable; furthermore, this code space encodes $n - 1$ qubits in $n$.

**Exercise 7.30** *Show that the $n$-qubit jump process of Section 7.5.1 follows by choosing, $\gamma = 0$ and $\hat{S} = X^{\otimes n}$, and that $\hat{D}_j = \kappa_j Z_j$.*

**Exercise 7.31** *Show that the $n$-qubit diffusion process in Section 7.5.1 follows by choosing, $\forall j, |\gamma_j| \to \infty$ and $\phi_j = \pi/2$.*
**Hint:** *See Ref. [AWM03].*

### 7.5.5 Other generalizations

In the above we have emphasized that it is always possible to choose one stabilizer, and so encode $n - 1$ qubits in $n$ qubits. However, there are situations in which one might choose a less efficient code with more than one stabilizer. In particular, it is possible to choose a stabilizer $\hat{S}_j$ for each error channel $\hat{c}_j$, with $\hat{S}_j \neq \hat{S}_k$ in general. For example, for the spontaneous emission errors $\hat{c}_j = X_j - \mathrm{i}Y_j$ one could choose $\hat{S}_j$ as particular stabilizers

[2] Strictly, this need not be a stabilizer group, since $\hat{S}$ need not be in the Pauli group, but the algebra is identical, so the analysis is unchanged.

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

of the universal five-qubit code. This choice is easily made, since the usual generators of the five-qubit code are $\{XZZXI, IXZZX, XIXZZ, ZXIXZ\}$ as discussed above. For each qubit $j$, we may pick from this set a stabilizer $\hat{S}_j$ that acts as $X$ on that qubit, since $X$ anticommutes with $\hat{D}_j = Z_j$.

In this case, since there are four stabilizer generators, only a single logical qubit can be encoded. However, this procedure would be useful in a system where spontaneous emission is only the dominant error process. If these errors could be detected (with a high degree of efficiency) then they could be corrected using the feedback scheme given above. Then other (rarer) errors, including missed spontaneous emissions, could be corrected using standard canonical error correction, involving measuring the stabilizer generators as explained in Section 7.4.2. The effect of missed emissions from detector inefficiency is discussed in Ref. [AWM03].

Another generalization, which has been investigated in Ref. [AWJ04], is for the case in which there is more than one decoherence channel per qubit, but they are all still able to be monitored with high efficiency. If there are at most *two* error channels per qubit then the encoding can be done with a single stabilizer (and hence $n-1$ logical qubits) just as above. If there are more than two error channels per qubit then in general two stabilizers are required. That is, one can encode $n-2$ logical qubits in $n$ physical qubits, requiring just one more physical qubit than in the previous case. The simplest example of this, encoding two logical qubits in four physical qubits, is equivalent to the well-known quantum erasure code [GBP97] which protects against qubit loss.

## 7.6 QEC using continuous feedback

We turn now, from correction of detected errors by feedback, to correction of undetected errors by conventional error correction. As explained in Section 7.4.2, this usually consists of projective measurement (of the stabilizer generators) at discrete times, with unitary feedback to correct the errors. Here we consider a situation of *continuous* error correction, which may be more applicable in some situations. That is, we consider continual weak measurement of the stabilizer generators, with Hamiltonian feedback to keep the system within the code space. This section is based upon Ref. [SAJM04].

For specificity, we focus on bit-flip errors for which the code words are given in Eq. (7.54), and we assume a diffusive unravelling of the measurement of the stabilizer generators. These measurements will have no effect when the system is in the code space and will give error-specific information when it is not. However, because the measurement currents are noisy, it is impossible to tell from the current in an infinitesimal interval whether or not an error has occurred in that interval. Therefore we do not expect Markovian feedback to be effective. Rather, we must filter the current to obtain information about the error syndrome.

The optimal filter for the currents in this case (and more general cases) has been determined by van Handel and Mabuchi [vHM05]. Since the point of the encoding is to make the quantum information invisible to the measurements, the problem reduces to a classical one of estimating the error syndrome. It is known in classical control theory as the Wonham filter

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

[Won64]. Here we are using the word ‘filter’ in the sense of Chapter 6: a way to process the currents in order to obtain information about the system (or, in this case, about the errors). The filtering process actually involves solving nonlinear coupled differential equations in which the currents appear as coefficients for some of the terms. As discussed in Chapter 6, it is difficult to do such processing in real time for quantum systems. This motivates the analysis of Ref. [SAJM04], which considered a non-optimal, but much simpler, form of filtering: a linear low-pass filter for the currents.

In this section we present numerical results from Ref. [SAJM04] showing that, in a suitable parameter regime, a feedback Hamiltonian proportional to the sign of the filtered currents can provide protection from errors. This is perhaps not surprising, because, as seen in Section 7.4, the information about the error syndrome is contained in the signatures of the stabilizer generator measurements (that is, whether they are plus or minus one), a quantity that is fairly robust under the influence of noise.

The general form of this continuous error-correcting scheme is similar to the discrete case. It has four basic elements.

1. Information is encoded using a stabilizer code suited to the errors of concern.
2. The stabilizer generators are monitored and a suitable smoothing of the resulting currents determined.
3. From consideration of the discrete error-correcting unitaries, a suitable feedback Hamiltonian that depends upon the signatures of the smoothed measurement currents is derived.
4. The feedback is added to the system dynamics and the average performance of the QEC scheme is evaluated.

Given $m$ stabilizer generators and $d$ errors possible on our system, the stochastic master equation describing the evolution of a system under this error correction scheme is

$$\begin{aligned} d\rho_c(t) = {} & \sum_{k=1}^{d} \gamma_k \mathcal{D}[\hat{E}_k]\rho_c(t)dt \\ & + \sum_{l=1}^{m} \kappa \mathcal{D}[\hat{M}_l]\rho_c(t)dt + \sqrt{\eta\kappa}\mathcal{H}[\hat{M}_l]\rho_c(t)dW_l(t) \\ & + \sum_{k=1}^{d} -iG_k(t)[\hat{F}_k, \rho_c(t)]dt. \end{aligned} \tag{7.95}$$

Note that we have set the system Hamiltonian, $\hat{H}$ (which allows for gate operations on the code space) to zero in (7.95). The first line describes the effects of the errors, where $\sqrt{\gamma_k}\hat{E}_k$ is the Lindblad operator for error $k$, with $\gamma_k$ a rate and $\hat{E}_k$ dimensionless. The second line describes the measurement of the stabilizers $\hat{M}_l$, with $\kappa$ the measurement rate (assumed for simplicity to be the same for all measurements). We also assume the same efficiency $\eta$ for all measurements so that the measurement currents $dQ_l/dt$ can be defined by

$$dQ_l = 2\kappa \,\mathrm{Tr}\big[\rho_c\hat{M}_l\big]dt + \sqrt{\kappa/\eta}\, dW_l. \tag{7.96}$$

The third line describes the feedback, with $\hat{F}_k$ a dimensionless Hermitian operator intended to correct error $\hat{E}_k$. Each $G_k$ is the feedback strength (a rate), a function of the smoothed (dimensionless) currents

$$R_l(t) = (1 - \mathrm{e}^{-rT})^{-1} \int_{t-T}^{t} r\mathrm{e}^{-r(t-t')}\,\mathrm{d}Q_l(t')/(2\kappa). \tag{7.97}$$

Here the normalization of this low-pass filter has been defined so that $R_l(t)$ is centred around ±1. We take $T$ to be moderately large compared with $1/r$.

In a practical situation the $\gamma_k$s are outside the experimenters' control (if they could be controlled, they would be set to zero). The other parameters, $\kappa$, $r$ and the characteristic size of $G_l$ (which we will denote by $\lambda$), can be controlled. The larger the measurement strength $\kappa$, the better the performance should be. However, as will be discussed in Section 7.6.1, in practice $\kappa$ will be set by the best available measurement device. In that case, we expect there to be a region in the parameter space of $r$ and $\lambda$ where this error-control scheme will perform optimally. This issue can be addressed using simulations.

To undertake numerical simulations, one needs to consider a particular model. The simplest situation to consider is protecting against bit-flips using the three-qubit bit-flip code of Section 7.4.2. We assume the same error rate for the three errors, and efficient measurements. This is described by the above SME (7.95), with $\gamma_k = \gamma$, $\eta = 1$, and

$$\hat{E}_1 = XII, \qquad \hat{E}_2 = IXI, \qquad \hat{E}_3 = IIX, \tag{7.98}$$

$$\hat{M}_1 = ZZI, \qquad \hat{M}_2 = IZZ. \tag{7.99}$$

A suitable choice for $\hat{F}_k$ is to set them equal to $\hat{E}_k$. Because the smoothed currents $R_l$ correspond to the measurement syndrome (the sign of the result of a strong measurement of $\hat{M}_l$), we want $G_k$ to be such that the following apply.

1. If $R_1(t) < 0$ and $R_2(t) > 0$, apply $XII$.
2. If $R_1(t) > 0$ and $R_2(t) < 0$, apply $IIX$.
3. If $R_1(t) < 0$ and $R_2(t) < 0$, apply $IXI$.
4. If $R_1(t) > 0$ and $R_2(t) > 0$, do not apply any feedback.

These conditions can be met by the following (somewhat arbitrary) choice:

$$G_1(t) = \begin{cases} \lambda R_1(t) & \text{if } R_1(t) < 0 \text{ and } R_2(t) > 0, \\ 0 & \text{otherwise,} \end{cases} \tag{7.100}$$

$$G_2(t) = \begin{cases} \lambda R_2(t) & \text{if } R_1(t) > 0 \text{ and } R_2(t) < 0, \\ 0 & \text{otherwise,} \end{cases} \tag{7.101}$$

$$G_3(t) = \begin{cases} \lambda R_1(t) & \text{if } R_1(t) < 0 \text{ and } R_2(t) < 0, \\ 0 & \text{otherwise.} \end{cases} \tag{7.102}$$

Recall that $\lambda$ is the characteristic strength of the feedback.

A numerical solution of the above SME was presented in Ref. [SAJM04]. As expected, it was found that the performance improved as $\kappa$ increased. Also it was found that the

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

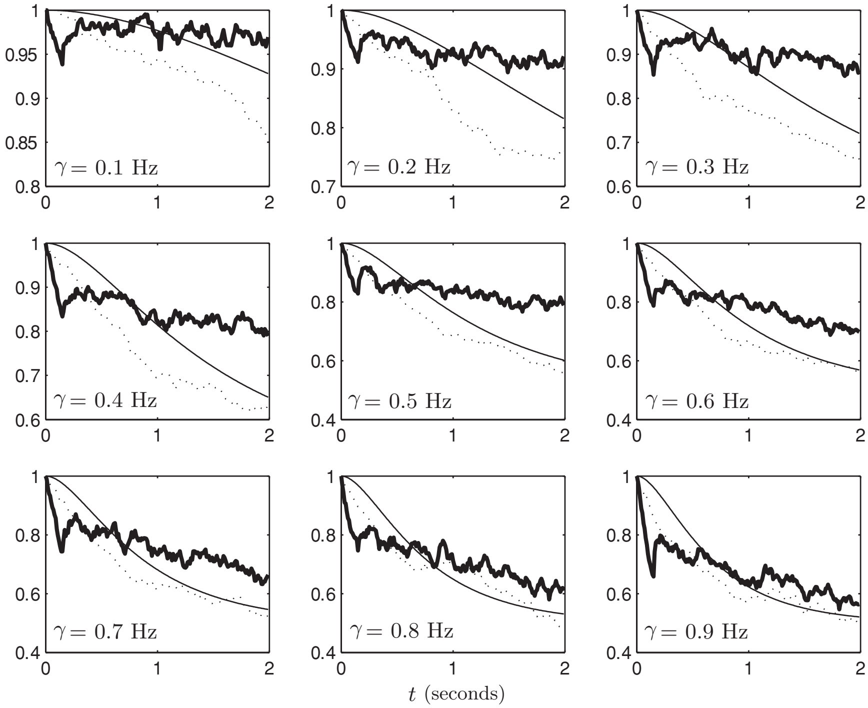

Fig. 7.6 Fidelity curves with and without error correction for several error rates $\gamma$. The thick solid curve is the average fidelity $F_3(t)$ of the three-qubit code with continuous error correction. The parameters used were $\mathrm{d}t = 10^{-4}$ s, $\kappa = 150\,\mathrm{s}^{-1}$, $\lambda = 150\,\mathrm{s}^{-1}$, $r = 20\,\mathrm{s}^{-1}$ and $T = 0.15$ s. The dotted curve is the average fidelity $F_1(t)$ of one qubit without error correction. The thin solid curve is the fidelity $F_{3d}(t)$ achievable by discrete QEC when the duration between applications is $t$. Figure 2 adapted with permission from M. Sarovar *et al.*, *Phys. Rev.* A **69**, 052324, (2004). Copyrighted by the American Physical Society.

optimum values of $r$ and $\lambda$ increase with $\kappa$, for $\gamma$ fixed. This is as expected, because the limit where $\kappa$, $r$ and $\lambda$ are large compared with $\gamma$ should approximate that of frequent strong measurements with correction. It was found that the best performance was achieved for $\lambda \geq \kappa$. However, as will be discussed in Section 7.6.1, in practice $\lambda$ may (like $\kappa$) be bounded above by the physical characteristics of the device. This would leave only one parameter ($r$) to be optimized.

The performance of this error-correction scheme can be gauged by the average fidelity $F_3(t)$ between the initial encoded three-qubit state and the state at time $t$ [SAJM04]. This is shown in Fig. 7.6 for several values of the error rate $\gamma$ (the time-units used are nominal; a discussion of realistic magnitudes is given in Section 7.6.1). Each plot also shows the fidelity curve $F_1(t)$ for one qubit in the absence of error correction. A comparison of these two curves shows that the fidelity is preserved for a longer period of time by the error-correction scheme for small enough error rates. Furthermore, for small error rates

($\gamma < 0.3\ \mathrm{s}^{-1}$) the $F_3(t)$ curve shows a great improvement over the exponential decay in the absence of error correction. However, we see that, past a certain threshold error rate, the fidelity decay even in the presence of error correction behaves exponentially, and the two curves look very similar; the error-correcting scheme becomes ineffective. In fact, well past the threshold, the fidelity of the (supposedly) protected qubit becomes lower than that of the unprotected qubit. This results from the feedback 'corrections' being so inaccurate that the feedback mechanism effectively increases the error rate.

The third line in the plots of Fig. 7.6 is of the average fidelity achievable by discrete QEC (using the same three-qubit code) when the time between the detection-correction operations is $t$. The value of this fidelity ($F_{3d}(t)$) as a function of time was analytically calculated in Ref. [ADL02] as

$$F_{3d} = \frac{1}{4}(2 + 3\mathrm{e}^{-2\gamma t} - \mathrm{e}^{-6\gamma t}). \tag{7.103}$$

A comparison between $F_3(t)$ and $F_{3d}(t)$ highlights the relative merits of the two schemes. The fact that the two curves cross each other for large $t$ indicates that, if the time between applications of discrete error correction is sufficiently large, then a continuous protocol will preserve fidelity better than a corresponding discrete scheme.

All the $F_3(t)$ curves show an exponential decay at very early times, $t \lesssim 0.1\,\mathrm{s}$. This is an artefact of the finite filter length and the specific implementation of the protocol in Ref. [SAJM04]: the simulations did not produce the smoothed measurement signals $R_l(t)$ until enough time had passed to get a full buffer of measurements. That is, feedback started only at $t = T$. We emphasize again that this protocol is by no means optimal.

The effect of non-unit efficiency $\eta$ was also simulated in Ref. [SAJM04], as summarized by Fig. 7.7. The decay of fidelity with decreasing $\eta$ indicates that inefficient measurements have a negative effect on the performance of the protocol as expected. However, the curves are quite flat for $1 - \eta$ small. This is in contrast to the correction of detected errors by Markovian feedback as considered in Section 7.5, where the rate of fidelity decay would be proportional to $1 - \eta$. This is because in the present case the measurement of the stabilizer generators has no deleterious effect on the encoded quantum information. Thus a reduced efficiency simply means that it takes a little longer to obtain the information required for the error correction.

### *7.6.1 Practical considerations for charge qubits*

Several schemes for solid-state quantum computing using the charge or spin degree of freedom of single particles as qubits, with measurements to probe this degree of freedom, have been proposed. Here we examine the weak measurement of one such proposed qubit: a single electron that can coherently tunnel between two quantum dots [HDW$^+$04]. The dots are formed by two P donors in Si, separated by a distance of about 50 nm. Surface gates are used to remove one electron from the double-donor system leaving a single electron on the P–P$^+$ system. This system can be regarded as a double-well potential. Surface gates

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

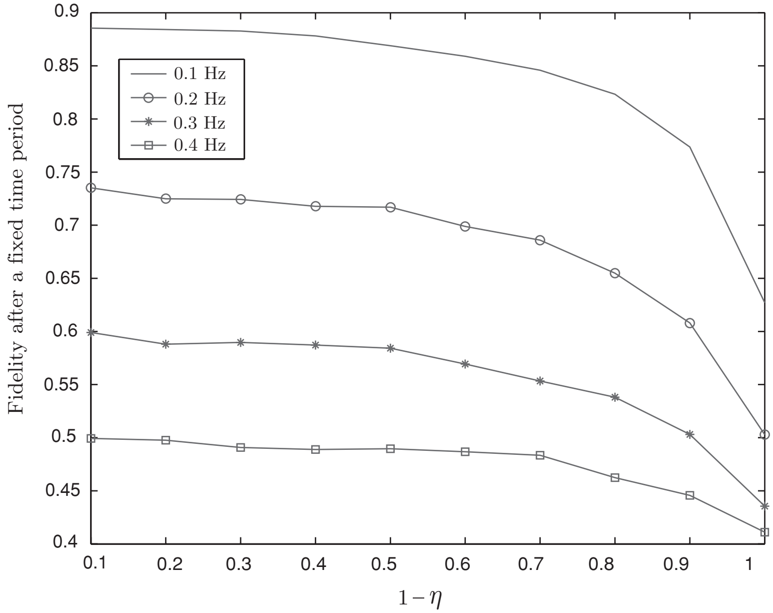

Fig. 7.7 Average fidelity after a fixed amount of time as a function of inefficiency $1 - \eta$ for several error rates. The parameters used were $\mathrm{d}t = 10^{-4}\,\mathrm{s}$, $\kappa = 50\,\mathrm{s}^{-1}$, $\lambda = 50\,\mathrm{s}^{-1}$, $r = 10\,\mathrm{s}^{-1}$ and $T = 0.15\,\mathrm{s}$. Figure 3 adapted with permission from M. Sarovar *et al.*, *Phys. Rev.* A **69**, 052324, (2004). Copyrighted by the American Physical Society.

can then be used to control the barrier between the wells, as well as the relative depth of the two wells. It is possible to design the double-well system so that, when the well depths are equal, there are only two energy eigenstates below the barrier. These states, $|+\rangle$ and $|-\rangle$, with energies $E_+$ and $E_-$, are symmetric and antisymmetric, respectively. The localized states describing the electron on the left or right of the barrier can thus be defined as

$$|L\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle), \tag{7.104}$$

$$|R\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle). \tag{7.105}$$

An initial state localized in one well will then tunnel to the other well at the frequency $\Delta = (E_+ - E_-)$.

Using $|L\rangle$ and $|R\rangle$ as the logical basis states $|0\rangle$ and $|1\rangle$, respectively, we can define Pauli matrices in the usual way. Then the Hamiltonian for the system can be well approximated by

$$\hat{H} = \frac{\omega(t)}{2}Z + \frac{\Delta(t)}{2}X. \tag{7.106}$$

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

A (time-dependent) bias gate can control the relative well depth $\omega(t)$ and similarly a barrier gate can control the tunnelling rate $\Delta(t)$. Further details on the validity of this Hamiltonian and how well it can be realized in the P–P$^+$ in Si system can be found in Ref. [BM03].

A number of authors have discussed the sources of decoherence in a charge qubit system such as this one [BM03, FF04, HDW$^+$04]. For appropriate donor separation, phonons can be neglected as a source of decoherence. The dominant sources are fluctuations in voltages on the surface gates controlling the Hamiltonian and electrons moving in and out of trap states in the vicinity of the dot. The latter source of decoherence is expected to dominate at low frequencies (long times), as for so-called $1/f$ noise. In any case, both sources can be modelled using the well-known spin–boson model (see Section 3.4.1) The key element of this model for the discussion here is that the coupling between the qubit and the reservoir is proportional to $Z$.

If the tunnelling term proportional to $\Delta(t)X$ in Eq. (7.106) were not present, decoherence of this kind would lead to pure dephasing. However, in a general single-qubit gate operation, both dephasing and bit-flip errors can arise in the spin–boson model. We use the decoherence rate calculated for this model as indicative for the bit-flip error rate in the toy model used above in which only bit-flips occur. Hollenberg *et al.* [HDW$^+$04] calculated that, for a device operating at 10 K, the error rate would be $\gamma = 1.4 \times 10^6\,\mathrm{s}^{-1}$. This rate could be made a factor of ten smaller by operating at lower temperatures and improving the electronics controlling the gates.

We now turn to estimating the measurement strength $\kappa$ for the P–P$^+$ system. In order to read out the qubit in the logical basis, we need to determine whether the electron is in the left or the right well quickly and with high probability of success. The technique of choice is currently based on radio-frequency single-electron transistors (RF-SETs) [SWK$^+$98]. A single-electron transistor is a very sensitive transistor whose operation relies upon single-electron tunneling onto and off a small metallic island (hence its name). That is, the differential resistance of the SET can be controlled by a very small bias voltage, which in this case arises from the Coulomb field associated with the qubit electron. Depending on whether the qubit is in the L or R state, this field will be different and hence the SET resistance will be different. In the RF configuration (which enables $1/f$ noise to be filtered from the signal) the SET acts as an Ohmic load in a tuned tank circuit. The two different charge states of the qubit thus produce two levels of power reflected from the tank circuit.

The electronic signal in the RF circuit carries a number of noise components, including amplifier noise, the Johnson noise of the circuit and ‘random telegraph’ noise in the SET bias conditions due to charges hopping randomly between charge trap states in or near the SET. The quality of the SET is captured by the minimum charge sensitivity per root hertz, $S$. In Ref. [BRS$^+$05] a value of $S \approx 5 \times 10^{-5} e/\sqrt{\mathrm{Hz}}$ was measured, for the conditions of observing the single-shot response to a charge change $\Delta q = 0.05e$. Here $e$ is the charge on a single electron, and $\Delta q$ means a change in the bias field for the SET corresponding to moving a charge of $\Delta q$ from its original position (on the P–P$^+$ system) to infinity. This is of order the field change expected for moving the electron from one P donor to the other. Thus the characteristic rate for measuring the qubit in the charge basis is of order $(\Delta q/S)^2 = 10^6\,\mathrm{Hz}$. Thus we take $\kappa\eta = 10^6\,\mathrm{s}^{-1}$. For definiteness we will say that $\eta = 1$

(that is, a quantum-limited measurement), even though that is almost certainly not the case (see for example Refs. [WUS+01, Goa03]). Note also that we are ignoring the difficulties associated with measuring stabilizers such as $ZZI$. That is, we simply use the one-qubit measurement rate for this joint multi-qubit measurement.

We next need to estimate typical values for the feedback strength. The feedback Hamiltonian is proportional to an $X$ operator, which corresponds to changing the tunnelling rate $\Delta$ for each of the double-dot systems that comprise each qubit. In Ref. [BM03], the maximum tunnelling rate was calculated to be about $10^9\,\mathrm{s}^{-1}$, for a donor separation of 40 nm. We take this to be the upper bound on $\lambda$.

To summarize, in the P–P$^+$-based charge qubit, with RF-SET readout, we have $\gamma \approx \kappa \approx 10^6\,\mathrm{s}^{-1}$ and $\lambda \lesssim 10^9\,\mathrm{s}^{-1}$. The fact that the measurement strength and the error rate are of the same order of magnitude for this architecture is a problem for our error-correction scheme. This means that the rate at which we gain information is about the same as the rate at which errors happen, and it is difficult to operate a feedback correction protocol in such a regime. Although it is unlikely that the measurement rate could be made significantly larger in the near future, as mentioned above it is possible that the error rate could be made smaller by improvements in the controlling electronics.

## 7.7 Continuous QEC without measurement

So far, both for discrete (as discussed in Section 7.4.2) and for continuous (as discussed in the preceding section) QEC, we have treated the measurement and control steps as involving a classical apparatus. However, as discussed in Section 1.3.1, measurement results can be stored in quantum systems and represented by quantum operators. Similarly, as discussed in Section 5.8.1, this information can be used to control the quantum systems that were measured by application of a suitable Hamiltonian. This suggests that it should be possible to implement the QEC process using only a few additional qubits, known as *ancilla* qubits. In other words, the entire process of detection and correction can be done with Hamiltonian dynamics and thus can be implemented with a quantum circuit.

A circuit that implements the three-qubit error-correction protocol without measurement is given in Fig. 7.8. In this circuit, the first three controlled-NOT gates effectively calculate the error syndrome (for the encoded state in the top three qubits), storing the result in the two ancilla qubits. Then the correction is done by direct coupling between the ancillae and the encoded qubits using Toffoli gates (doubly controlled-NOT gates). It is important to note that the ancilla qubits must be reset to the $|0\rangle$ state after each run of the circuit. This is a consequence of the fact that the entropy generated by the errors is moved into the ancilla subsystem and must be carried away before the next run of the circuit.

This circuit illustrates the essential ideas behind implementing error correction without measurement: introduction of ancilla qubits, their direct coupling to the encoded qubits, and the resetting of these ancilla qubits after each cycle. If this cycle comprising detect, correct and reset is performed often enough, and the only errors in our system are independent bit-flip errors at randomly distributed times, then one can preserve the value of a logical

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

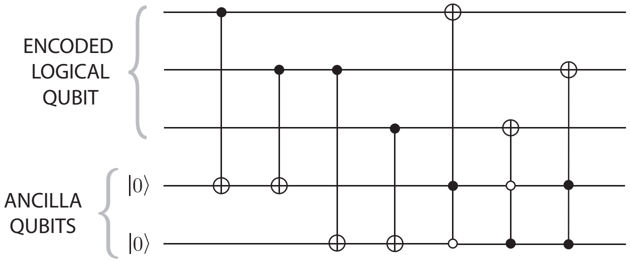

Fig. 7.8 A circuit for implementing error correction using the three-qubit bit-flip code without measurement. The top three qubits form the encoded logical qubit and the bottom two form the ancilla. The first four gates are C-NOT gates as described in Section 7.4.1. The last three are Toffoli gates, which are similar but have two controls (shown by the open or filled circles). The target (large encircled cross) undergoes a bit-flip iff the controls have the appropriate value (zero for an open circle, one for a filled circle). Note that, to repeat the error-correction procedure, the ancilla qubits must be replaced or reset to the $|0\rangle$ state at the end of each run (at the far right of the circuit). Figure 1 adapted with permission from M. Sarovar and G. J. Milburn, *Phys. Rev.* A **72**, 012306, (2005). Copyrighted by the American Physical Society.

qubit indefinitely. Note that we are assuming that the operations involved in the circuit – the unitary gates and the ancilla reset – are instantaneous. In this section we address the obvious question: can we replace these instantaneous discrete operations by continuous processes? That is, can we use a finite apparatus to obtain a continuous version of 'coherent' QEC (see Section 5.8.1) just as there are continuous versions of conventional QEC with measurement as discussed in Section 7.6?

The answer to this question is yes, as shown in Ref. [SM05]. Following that reference, we need to modify two components of the circuit model.

1. The unitary gates which form the system–ancilla coupling are replaced by a finite-strength, time-independent Hamiltonian. This Hamiltonian will perform both the detection and the correction operations continuously and simultaneously.
2. The ancilla reset procedure is replaced by the analogous continuous process of *cooling*. Each ancilla qubit must be independently and continuously cooled to its ground state $|0\rangle$.

These changes lead to a continuous-time description of the process in terms of a Markovian master equation, under the assumption that both open-system components – the errors and the ancilla cooling – are Markovian processes.

We illustrate this continuous-time implementation for the three-qubit bit-flip code example used previously. The continuous time description of the circuit of Fig. 7.8 is

$$\begin{aligned}\frac{d\rho}{dt} &= \gamma(\mathcal{D}[XIIII] + \mathcal{D}[IXIII] + \mathcal{D}[IIXII])\rho \\ &\quad + \lambda(\mathcal{D}[IIIL^\dagger I] + \mathcal{D}[IIIIL^\dagger])\rho - i\kappa[\hat{H}, \rho]. \end{aligned} \tag{7.107}$$

Here, the ordering of the tensor product for all operators in the equation runs down the circuit as shown in Fig. 7.8 (i.e. the first three operators apply to the encoded qubit and

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

the last two to the ancilla), while $L \equiv \frac{1}{2}(X + iY) = |1\rangle\langle 0|$ is a qubit lowering operator as before. The parameters are $\gamma$, the bit-flip error rate; $\kappa$, the strength of the coherent detection and correction (the Hamiltonian operator $\hat{H}$ is dimensionless); and $\lambda$, the rate of the cooling applied to the ancilla qubits.

To construct the dimensionless Hamiltonian in Eq. (7.107), we first determine Hamiltonians $\hat{H}_D$ and $\hat{H}_C$ that perform the detection and correction operations, respectively. The detection Hamiltonian is given by

$$\hat{H}_D = \hat{D}_1 \otimes (XI) + \hat{D}_2 \otimes (XX) + \hat{D}_3 \otimes (IX). \tag{7.108}$$

Here, $\hat{D}_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$ is the projector onto the subspace where there has been a bit-flip error on the first physical qubit, and $\hat{D}_2$ and $\hat{D}_3$ similarly for the second and third physical qubits. These operators act on the three qubits encoding the logical qubit, while the Pauli operators cause the appropriate bit-flips in the ancilla qubits. Similarly, the correction Hamiltonian is

$$\hat{H}_C = \hat{C}_1 \otimes (PI) + \hat{C}_2 \otimes (PP) + \hat{C}_3 \otimes (IP). \tag{7.109}$$

Here $P \equiv (1 - Z)/2 = |1\rangle\langle 1|$, the projector onto the logical one state of a qubit. We have also defined $\hat{C}_1 = X \otimes (|00\rangle\langle 00| + |11\rangle\langle 11|)$, an operator that corrects a bit-flip on the first physical qubit (assuming that the second and third remain in the code space), and $\hat{C}_2$ and $\hat{C}_3$ similarly for the second and third physical qubits.

The operation in Fig. 7.8 of detection followed by correction can be realized by the unitary $\hat{U}_{DC} = \exp(-i\hat{H}_C\pi/2)\exp(-i\hat{H}_D\pi/2)$.

**Exercise 7.32** *Verify this.*

Now, by the Baker–Campbell–Hausdorff theorem (A.118), it follows that the unitary $\hat{U}_{DC}$ has a generator of the form

$$\hat{H} = \hat{H}_D + \hat{H}_C + i\alpha[\hat{H}_D, \hat{H}_C], \tag{7.110}$$

for some $\alpha$. That is, $\ln(\hat{U}_{DC}) \propto -i\hat{H}$.

**Exercise 7.33** *Verify this.*
**Hint:** *Show that* $\{\hat{H}_C, \hat{H}_D, i[\hat{H}_D, \hat{H}_C]\}$ *form a Lie algebra (see Box 6.2).*

Although it would be possible to determine $\alpha$ from the above argument, it is more fruitful to consider it as a free parameter in $\hat{H}$. That is because the above argument is just a heuristic to derive a suitable $\hat{H}$, since the circuit model does not have the cooling process simultaneous with the detection and correction. It was shown in Ref. [Sar06] that good results were obtained with $\alpha = 1$, and this is the value used in Ref. [SM05].

Note that in Eq. (7.107) the error processes are modelled only on qubits that form the encoded state. One could extend the error dynamics on to the ancilla qubits. However, in the parameter regime where the error correction is effective, $\lambda \gg \gamma$, the cooling will dominate all other ancilla dynamics. Thus we can ignore the error dynamics on the ancilla qubits.

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

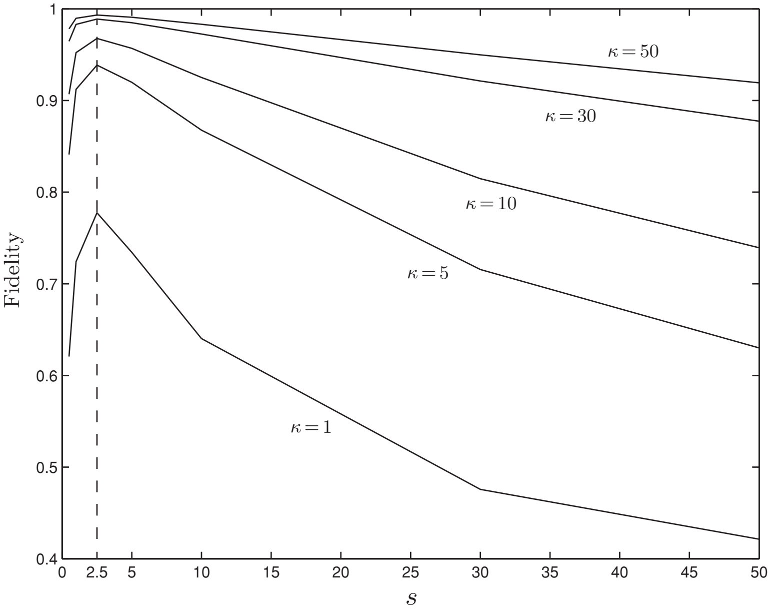

Fig. 7.9 Fidelity, after a fixed period of time ($T = 10$), of an encoded qubit (three-qubit code) undergoing continuous error correction using cooled ancillae. Here time is measured in arbitrary units, with $\gamma = 1/20$. The curves are for different Hamiltonian strengths ($\kappa$) and the horizontal axis shows how the cooling rate is scaled with $\kappa$; i.e. $\lambda = s\kappa$, where $s$ is varied along the horizontal axis. Figure 2 adapted with permission from M. Sarova and G. J. Milburn, *Phys. Rev.* A **72**, 012306, (2005). Copyrighted by the American Physical Society.

In Ref. [SM05], Eq. (7.107) was solved by numerical integration and the fidelity $F(t) \equiv \langle\psi|\rho(t)|\psi\rangle$ determined. Here $\rho(t)$ is the reduced state of the encoded subsystem and $\rho(0) = |\psi\rangle\langle\psi|$ is the initial logical state. For a given error rate $\gamma$ we expect there to be an optimal ratio between the Hamiltonian strength $\kappa$ and the cooling rate $\lambda$. Figure 7.9 shows the fidelity after a fixed period of time $1/(2\gamma)$ for several values of these parameters, and it is clear that the best performance is when $\lambda \approx 2.5\kappa$. This optimal point is independent of the ratio of $\kappa$ to $\gamma$ and of the initial state of the encoded qubits. The following results were all obtained in this optimal parameter regime.

Figure 7.10 shows the evolution of fidelity with time for a fixed error rate and several values of $\kappa$. This clearly shows the expected improvement in performance with an increase in the Hamiltonian strength. Large values of $\kappa$ and $\lambda$ are required in order to maintain fidelity at reasonable levels. To maintain the fidelity above 0.95 up to time $T = 1/(2\gamma)$ requires $\kappa/\gamma > 200$. However, a comparison with the unprotected qubit's fidelity curve shows a marked improvement in coherence, due to the error-correction procedure. Therefore, implementing error correction even in the absence of ideal resources is valuable. This was also evident in the scenario of error correction *with* measurement in the preceding section.

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

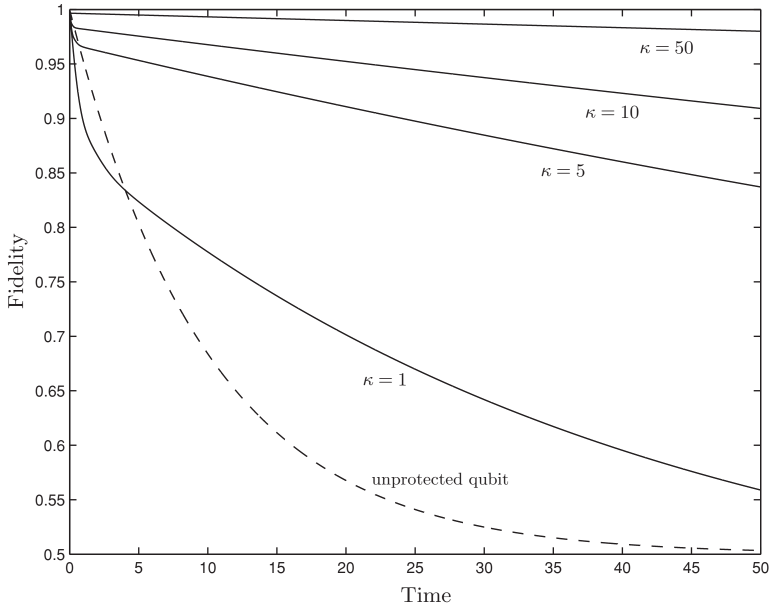

Fig. 7.10 Fidelity curves for several Hamiltonian strengths versus time. Time is measured in arbitrary units, with $\gamma = 1/20$. The solid curves are the fidelity of an encoded qubit (three-qubit code) with continuous error correction. The dashed curve is the fidelity of one qubit undergoing random bit-flips without error correction. Figure 3 adapted with permission from M. Sarovar and G. J. Milburn, *Phys. Rev.* A **72**, 012306, (2005). Copyrighted by the American Physical Society.

Aside from describing a different implementation of error correction, the scheme above casts error correction in terms of the very natural process of cooling; it refines the viewpoint that error correction extracts the entropy that enters the system through errors. Error correction is not cooling to a particular state such as a ground state, but rather a subspace of Hilbert space, and the specially designed coupling Hamiltonian allows us to implement this cooling to a (nontrivial) subspace by a simple cooling of the ancilla qubits to their ground state.

## 7.8 Linear optical quantum computation

### *7.8.1 Measurement-induced optical nonlinearity*

One of the earliest proposals [Mil89] for implementing quantum computation was based on encoding a single qubit as a single-photon excitation of an optical field mode. The qubits were assumed to interact via a medium with a nonlinear refractive index, such as discussed in Section 5.3. However, it is extremely difficult to implement a significant unitary coupling between two optical modes containing one or two photons. In 2001, Knill *et al.* [KLM01] discovered an alternative approach based on how states change due to measurement. They

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

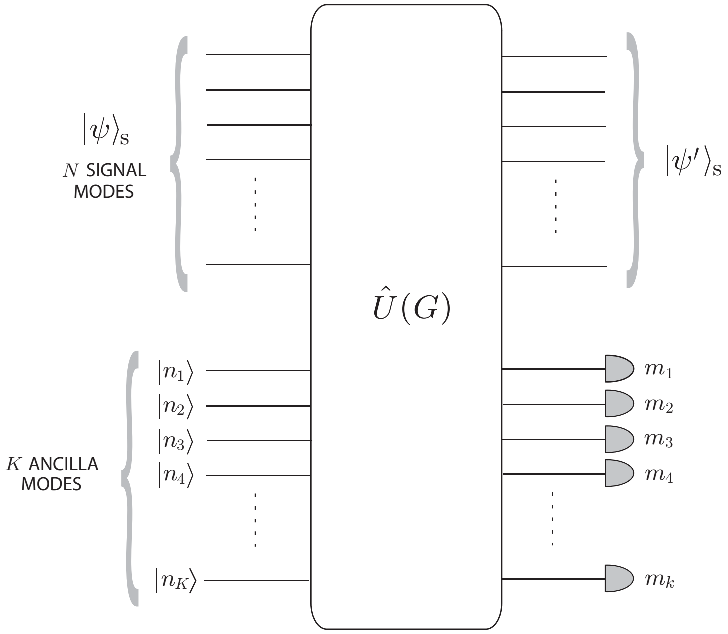

Fig. 7.11 A general conditional linear optical gate.

showed that non-deterministic photonic qubit gates are possible with linear optical networks when some of the input modes (referred to as *ancilla* modes) are prepared in single-photon states before the optical network and directed to photon counters at the network output. The conditional state of all non-ancilla modes (the *signal* modes), conditioned on a particular count on the output ancilla modes, is given by a non-unitary transformation of the input signal state and can simulate a highly nonlinear optical process. This transformation is defined in terms of a conditional measurement operator acting on the signal modes alone.

Consider the situation depicted in Fig. 7.11. In this device $N + K$ modes pass through a linear optical device, comprising only mirrors and beam-splitters. We describe this by a unitary transformation (that is, we ignore losses through absorption etc.) so that the total photon-number is conserved. The $K$ ancilla modes are prepared in photon-number eigenstates. At the output, photon-number measurements are made on the ancilla modes alone. We seek the *conditional* state for the remaining $N$ modes, *given* the ancilla photon-number count.

The linear optical device performs a unitary transformation on all the input states:

$$\hat{U}(G) = \exp[-\mathrm{i}\hat{\mathbf{a}}^{\dagger} G\, \hat{\mathbf{a}}], \tag{7.111}$$

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

where $\mathbf{\hat{a}}$ is a vector of annihilation operators,

$$\mathbf{\hat{a}} = \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \\ \vdots \\ \hat{a}_N \\ \hat{a}_{N+1} \\ \vdots \\ \hat{a}_{N+K} \end{pmatrix}, \tag{7.112}$$

and $G$ is an Hermitian *matrix* (not an operator). This transformation induces a unitary transform on the vector $\mathbf{\hat{a}}$:

$$\hat{U}^\dagger(G)\mathbf{\hat{a}}\,\hat{U}(G) = S(G)\mathbf{\hat{a}}. \tag{7.113}$$

One should not confuse the unitary transformation $\hat{U}(G)$ (an operator) with the induced unitary representation $S(G) = \exp(-\mathrm{i}G)$ (a matrix). Because $S(G)$ is unitary, the transformation leaves the total photon number invariant:

$$\hat{U}^\dagger(G)\mathbf{\hat{a}}^\dagger\mathbf{\hat{a}}\,\hat{U}(G) = \mathbf{\hat{a}}^\dagger S(G)S(G)^\dagger\mathbf{\hat{a}} = \mathbf{\hat{a}}^\dagger\mathbf{\hat{a}}. \tag{7.114}$$

Remember that, as in Chapter 6, $\mathbf{\hat{a}}^\dagger = (\hat{a}_1^\dagger, \ldots, \hat{a}_{N+K}^\dagger)$, so that $\mathbf{\hat{a}}^\dagger\mathbf{\hat{a}} = \sum_k \hat{a}_k^\dagger\hat{a}_k$.

**Exercise 7.34** *Verify that* $S(G) = \exp(-\mathrm{i}G)$.
**Hint:** *Show that, for a Hamiltonian* $\mathbf{\hat{a}}^\dagger G\,\mathbf{\hat{a}}$, $\mathrm{d}\mathbf{\hat{a}}/\mathrm{d}t = -\mathrm{i}G\mathbf{\hat{a}}$.

The *conditional state* of the signal modes, $|\psi'\rangle_{\mathrm{s}}$, is determined by

$$|\psi'\rangle_{\mathrm{s}} = \frac{1}{\sqrt{\wp(\vec{m})}}\hat{M}(\vec{m}|\vec{n})|\psi\rangle_{\mathrm{s}}. \tag{7.115}$$

Here the observed count is represented by the vector of values $\vec{m}$, and the probability for this event is $\wp(\vec{m})$. The measurement operator is

$$\hat{M}(\vec{n}|\vec{m}) = {}_{\mathrm{anc}}\langle\vec{m}|\hat{U}(G)|\vec{n}\rangle_{\mathrm{anc}} \tag{7.116}$$

with

$$|\vec{m}\rangle_{\mathrm{anc}} = |m_1\rangle_{N+1} \otimes |m_2\rangle_{n+2} \otimes \ldots \otimes |m_k\rangle_{N+K}. \tag{7.117}$$

As an example consider a three-mode model defined by the transformation

$$S(G)\mathbf{\hat{a}} = \begin{pmatrix} s_{11} & s_{12} & s_{13} \\ s_{21} & s_{22} & s_{23} \\ s_{31} & s_{32} & s_{33} \end{pmatrix}\begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \\ \hat{a}_3 \end{pmatrix}. \tag{7.118}$$

We will regard $\hat{a}_2$ and $\hat{a}_3$ as the ancilla modes, prepared in the single-photon state $|1, 0\rangle$. That is, $n_2 = 1$ and $n_3 = 0$. We will condition on a count of $m_2 = 1$ and $m_3 = 0$. We want

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

the two-mode conditional measurement operator $\hat{M}(1,0|1,0)$ acting on mode $\hat{a}_1$. Since photon number is conserved, the only non-zero elements of this operator are

$$\begin{aligned}\langle n|\hat{M}(1,0|1,0)|n\rangle &= \langle n,1,0|\hat{U}(G)|n,1,0\rangle \\ &= (n!)^{-1}\langle 0,0,0|\hat{a}_1^n\hat{a}_2\hat{U}(G)(\hat{a}_1^\dagger)^n\hat{a}_2^\dagger|0,0,0\rangle.\end{aligned} \tag{7.119}$$

This expression simplifies to

$$\frac{1}{n!}\langle 0,0,0|(s_{11}\hat{a}_1+s_{12}\hat{a}_2+s_{13}\hat{a}_3)^n(s_{21}\hat{a}_1+s_{22}\hat{a}_2+s_{23})\hat{a}_3(\hat{a}_1^\dagger)^n\hat{a}_2^\dagger|0,0,0\rangle. \tag{7.120}$$

**Exercise 7.35** *Show this, and also show that, since $\hat{a}_3^\dagger$ does not appear in Eq. (7.120), further simplification is possible, namely to*

$$(n!)^{-1}\langle 0,0,0|(s_{11}\hat{a}_1+s_{12}\hat{a}_2)^n(s_{21}\hat{a}_1+s_{22}\hat{a}_2)(\hat{a}_1^\dagger)^n\hat{a}_2^\dagger|0,0,0\rangle. \tag{7.121}$$

**Hint:** *First show that $\langle 0,0,0|\hat{U}^\dagger(G)=\langle 0,0,0|$, and so replace $\hat{a}_1^n\hat{a}_2\hat{U}(G)$ by $\hat{U}^\dagger(G)\hat{a}_1^n\hat{a}_2\hat{U}(G)$.*

From this it can be shown that a formal expression for $\hat{M}(10|10)$ is

$$\hat{M}(1,0|1,0)=s_{12}s_{21}\hat{a}_1^\dagger\hat{A}\hat{a}_1+s_{22}\hat{A}, \tag{7.122}$$

where $\hat{A}=\sum_{n=0}^{\infty}(s_{11}-1)^n(\hat{a}_1^\dagger)^n\hat{a}_1^n/n!$. We will not use this expression directly. However, it does serve to emphasize the optical nonlinearity in the measurement, since it contains all powers of the field operator.

### *7.8.2 Two-qubit gates*

The above non-deterministic transformations can be used for universal quantum computation. This scheme and others like it are called linear optical quantum computation (LOQC) schemes. Universal quantum computation [NC00] can be achieved if one can perform arbitrary single-qubit unitaries, and implement a two-qubit entangling gate (such as the C-NOT gate), between any two qubits. In order to see how these one- and two-qubit gates are possible in LOQC, we need to specify a physical encoding of the qubit. In this section we use a 'dual-rail' logic based on two modes and one photon:

$$|0\rangle_L = |1\rangle_1\otimes|0\rangle_2, \tag{7.123}$$

$$|1\rangle_L = |0\rangle_1\otimes|1\rangle_2. \tag{7.124}$$

The modes could be distinguished spatially (e.g. a different direction for the wave vector), or they could be distinguished by polarization.

One single-qubit gate that is easily implemented uses a beam-splitter (for spatially distinguished modes) or a wave-plate (for modes distinguished in terms of polarization). These linear optical elements involving two modes can be described by the unitary transformation

$$\hat{U}(\theta)=\exp\Big[-\mathrm{i}\theta(\hat{a}_1^\dagger\hat{a}_2+\hat{a}_1\hat{a}_2^\dagger)\Big], \tag{7.125}$$

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

which coherently transfers excitations from one mode to the other. Another simple single-qubit gate is a relative phase shift between the two modes, which can be achieved simply by altering the optical path-length difference. For spatially distinguished modes this can be done by altering the actual length travelled or using a thickness of refractive material (e.g. glass), whereas for polarization-distinguished modes, a thickness of birefringent material (e.g. calcite) can be used. This gate can be modelled by the unitary $\hat{U}(\phi) = \exp\left[-\mathrm{i}(\phi/2)(\hat{a}_1^\dagger\hat{a}_1 - \hat{a}_2^\dagger\hat{a}_2)\right]$.

**Exercise 7.36** *Show that $X = \hat{a}_1^\dagger\hat{a}_2 + \hat{a}_1\hat{a}_2^\dagger$ and $Z = \hat{a}_1^\dagger\hat{a}_1 - \hat{a}_2^\dagger\hat{a}_2$ act as the indicated Pauli operators on the logical states defined above.*

By concatenating arbitrary rotations around the $X$ and $Z$ axes of the Bloch sphere of the qubit, one is able to implement arbitrary single-qubit gates.

**Exercise 7.37** *Convince yourself of this.*
**Hint:** *For the mathematically inclined, consider the Lie algebra generated by $X$ and $Z$ (see Section 6.6.2). For the physically inclined, think about rotating an object in three-dimensional space.*

A simple choice for an entangling two-qubit gate is the conditional sign-change (CS) gate. In the logical basis it is defined by

$$|x\rangle_L|y\rangle_L \to \mathrm{e}^{\mathrm{i}\pi x\cdot y}|x\rangle_L|y\rangle_L. \qquad (7.126)$$

This was the sort of interaction considered in Ref. [Mil89], in which the logical basis was the photon-number basis. It is then implementable by a so called mutual-Kerr-effect nonlinear phase shift:

$$\hat{U}_{\text{Kerr}} = \exp[\mathrm{i}\pi a_1^\dagger a_1 a_2^\dagger a_2]. \qquad (7.127)$$

This requires the photons to interact via a nonlinear medium. In practice it is not possible to get a single-photon phase shift of $\pi$, which this transformation implies, without adding a considerable amount of noise from the medium. However, as we now show, we can realize a CS gate non-deterministically using the dual-rail encoding and the general method introduced in the preceding subsection.

With dual-rail encoding, a linear optical network for a two-qubit gate will have, at most, two photons in any mode. As we will show later, the CS gate can be realized if we can realize the following transformation on a single mode in an arbitrary superposition of no, one and two photons:

$$|\psi\rangle = \alpha_0|0\rangle_1 + \alpha_1|1\rangle_1 + \alpha_2|2\rangle_1 \to |\psi'\rangle = \alpha_0|0\rangle_1 + \alpha_1|1\rangle_1 - \alpha_2|2\rangle_1, \qquad (7.128)$$

with success probability independent of $\alpha_n$. We will refer to this as a nonlinear sign-change gate (NS gate).

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

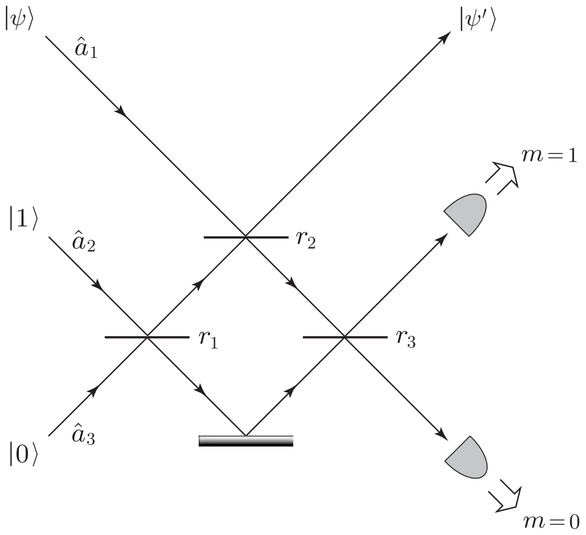

Fig. 7.12 The NS gate $|\psi\rangle \rightarrow |\psi'\rangle$ constructed from three beam-splitters with reflectivities of $r_i = \sin\theta_i$ with $\theta_1 = \theta_3 = 22.5^\circ$, $\theta_2 = 114.47^\circ$. Adapted by permission from Macmillan Publishers Ltd: *Nature*, E. Knill *et al.*, **409**, 46, Figure 1, copyright 2001.

The NS gate can be achieved using the measurement operator $\hat{M}(10, 10)$ of Eq. (7.122). From Eq. (7.121), for $n \in \{0, 1, 2\}$, we require

$$\begin{aligned} s_{22} &= \lambda, \\ s_{22}s_{11} + s_{12}s_{21} &= \lambda, \\ 2s_{11}s_{12}s_{21} + s_{22}s_{11}^2 &= -\lambda, \end{aligned}$$

for some complex number $\lambda$. The phase of $\lambda$ corresponds to an unobservable global phase shift, while $|\lambda|^2$ is the probability of the measurement outcome under consideration. One solution is easily verified to be

$$S = \begin{pmatrix} 1-2^{1/2} & 2^{-1/4} & (3/2^{1/2}-2)^{1/2} \\ 2^{-1/4} & 1/2 & 1/2-1/2^{1/2} \\ (3/2^{1/2}-2)^{1/2} & 1/2-1/2^{1/2} & 2^{1/2}-1/2 \end{pmatrix}. \tag{7.129}$$

Here $\lambda = 1/2$, so the success probability is $1/4$. This is the best that can be achieved in a linear optical system via a non-deterministic protocol without some kind of feedforward protocol [Eis05]. An explicit linear optical network to realize this unitary transformation $S$ using three beam-splitters is shown in Fig. 7.12.

In Fig. 7.13, we show how two non-deterministic NS gates can be used to implement a CS gate in dual-rail logic. Here the beam-splitters are all 50 : 50 ($\theta = \pi/4$). Since success requires both the NS gates to work, the overall probability of success is $1/16$. A simplification of this scheme that uses only two photons was proposed by Ralph *et al.* [RLBW02].

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

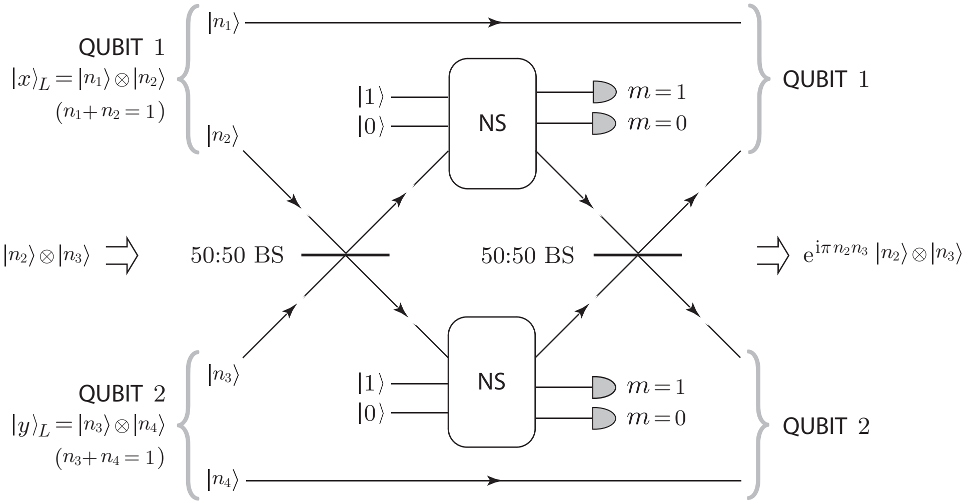
QUBIT 1
$|x\rangle_L = |n_1\rangle \otimes |n_2\rangle$
$(n_1 + n_2 = 1)$
$|n_1\rangle$
$|n_2\rangle$
$|1\rangle$
$|0\rangle$
NS
$m=1$
$m=0$
QUBIT 1
$|n_2\rangle \otimes |n_3\rangle \Rightarrow$
50:50 BS
50:50 BS
$\Rightarrow e^{i\pi n_2 n_3} |n_2\rangle \otimes |n_3\rangle$
QUBIT 2
$|y\rangle_L = |n_3\rangle \otimes |n_4\rangle$
$(n_3 + n_4 = 1)$
$|n_3\rangle$
$|n_4\rangle$
$|1\rangle$
$|0\rangle$
NS
$m=1$
$m=0$
QUBIT 2

Fig. 7.13 A CS two-qubit gate implemented using two non-deterministic NS gates. This gate has no effect on the two-qubit input state, except to change the sign of the $|1\rangle|1\rangle$ component, as indicated. Adapted by permission from Macmillan Publishers Ltd: *Nature*, E. Knill *et al.*, **409**, 46, Figure 1, copyright 2001.

It is simplified first by setting the beam-splitter parameters $r_1$ and $r_3$ to zero in the NS gate implementation (Fig. 7.12), and second by detecting exactly one photon at each logical qubit output. The device is non-deterministic and succeeds with probability of $1/9$, but is not scalable insofar as success is heralded by the coincident detection of both photons at distinct detectors: failures are simply not detected at all. It is this simplified gate that was the first to be experimentally realized in 2003 [OPW$^+$03], and it has become the work-horse for LOQC experiments [KMN$^+$07].

### *7.8.3 Teleporting to determinism*

A cascaded sequence of non-deterministic gates is useless for quantum computation because the probability of many gates working in sequence would decrease exponentially. This problem may be avoided by using a protocol based on qubit teleportation as described in Section 7.2. In essence we hold back the gate until we are sure it works and then teleport it on to the required stage of the computation.

The idea that teleportation can be used for universal quantum computation was first proposed by Gottesman and Chuang [GC99]. The idea is to prepare a suitable entangled state for a teleportation protocol with the required gate already applied. We illustrate the idea for teleporting a C-NOT gate in Fig. 7.14. Consider two qubits in an unentangled pure state $|\alpha\rangle \otimes |\beta\rangle$ as shown in Fig. 7.14. Now, to teleport these two qubits one can simply teleport them separately, using two copies of the Bell state $|\psi\rangle$ with measurements and feedforward as introduced in Section 7.2. Now say that, before performing the teleportation protocol,

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

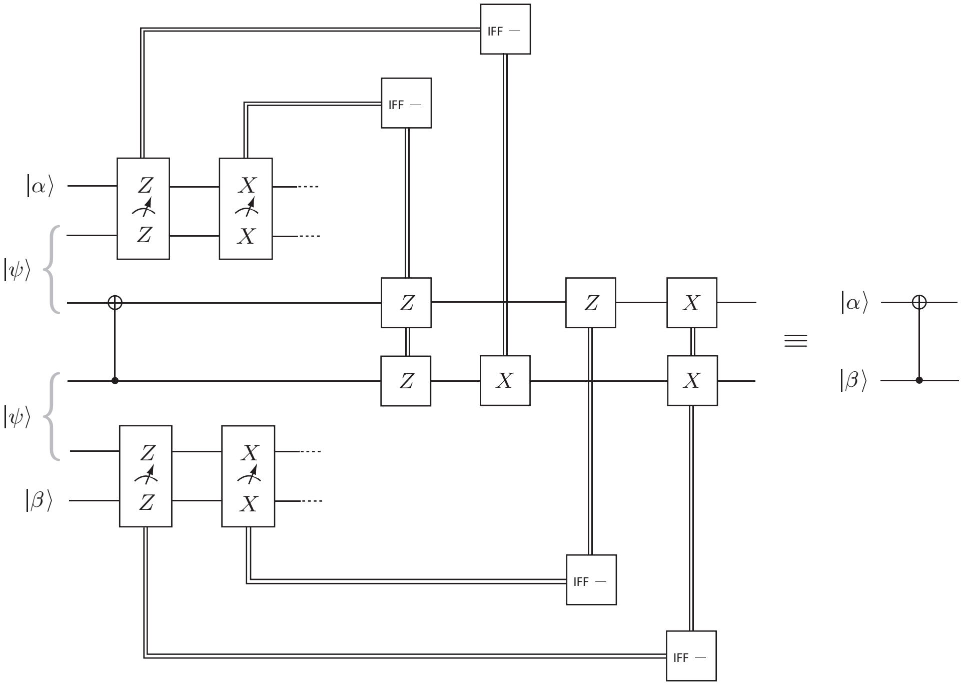

Fig. 7.14 Quantum teleportation of a C-NOT gate on to the state $|\alpha\rangle \otimes |\beta\rangle$ (with $|\beta\rangle$ being the control). The C-NOT at the start of the circuit can be considered part of the preparation of the entangled resource used in the teleportation, which can be discarded and reprepared if this C-NOT fails. Other details are as in Fig. 7.1.

we implement a C-NOT gate between two qubits in the four-qubit state $|\psi\rangle \otimes |\psi\rangle$ – the two qubits that will carry the teleported state. The result is to produce an entangled state (in general) at the output of the dual-rail teleporter, rather than the product state $|\alpha\rangle \otimes |\beta\rangle$. Moreover, by modifying the controls applied in the teleportation protocol the device can be made to output a state that is identical to that which would have been obtained by applying a C-NOT gate directly on the state $|\alpha\rangle \otimes |\beta\rangle$ (with $|\beta\rangle$ being the control).

**Exercise 7.38** *Verify that the circuit in Fig. 7.14 works in this way.*

This teleportation of the C-NOT gate works regardless of the initial state of the two qubits. As dicussed above, the C-NOT gate can be realized using a non-deterministic NS gate. The point of the teleportation protocol is that, if it fails, we simply repeat the procedure with another two entangled states $|\psi\rangle \otimes |\psi\rangle$, until the preparation succeeds. When it has succeeded, we perform the protocol in Fig. 7.14. Note that the entangled state $|\psi\rangle$ can also be prepared non-deterministically using a NS gate.

There is one remaining problem with using teleportation to achieve two-qubit gates in LOQC: it requires the measurement of the operators $XX$ and $ZZ$ on a pair of qubits. This

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

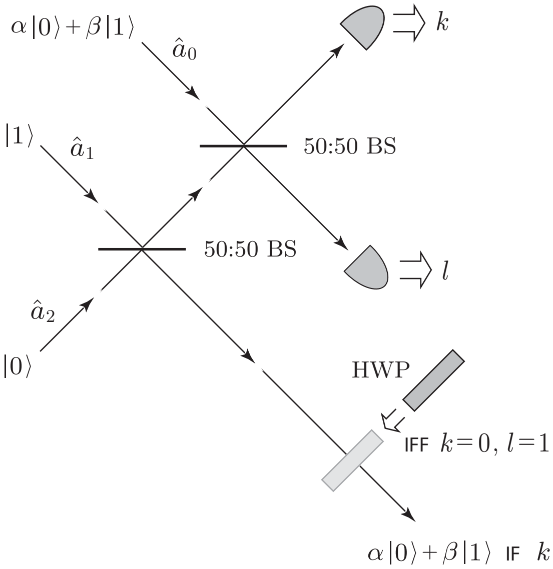

Fig. 7.15 A simple non-deterministic teleportation protocol. The protocol works whenever the total count at the output photon counters is unity.

can be achieved with these two qubits alone, using only single-qubit unitaries, single-qubit measurements in the logical basis and two applications of a C-NOT gate.

**Exercise 7.39** *Try to construct the circuit that achieves this using the resources described.*

The problem is that the C-NOT itself is a two-qubit gate! It would seem that this would lead to an infinite regress, with an ever-decreasing probability of success. However, it can be shown that, by using the appropriate entangled resource, the teleportation step can be made near-deterministic. This near-deterministic teleportation protocol requires only photon counting and the ability to perform local quantum control on the basis of these measurement results.

Figure 7.15 shows the basic LOQC quantum teleportation protocol. Note that the states $|0\rangle$ and $|1\rangle$ here are photon-number states, not the dual-rail encoded logical states introduced in Section 7.8.2. That is, the teleporter actually works on a 'single-rail' qubit $|\phi\rangle = \alpha|0\rangle_0 + \beta|1\rangle_0$, transferring it from mode $a_0$ to mode $a_2$. A dual-rail qubit can be teleported by teleporting the two single-rail qubits in its two modes. In Section 7.9 we will consider LOQC based on single-rail qubits, for which the teleportation scheme of Fig. 7.15 can be used directly.

The teleportation scheme begins by preparing the ancilla state $|\psi\rangle = (|01\rangle_{12} + |10\rangle_{12})/\sqrt{2}$. In terms of single-rail qubits in modes 1 and 2, this is an entangled state. We denote it $|t_1\rangle_{12}$, because it is a teleportation resource that can be created by sharing one photon between modes 1 and 2, simply using a beam-splitter as shown in Fig. 7.15. A second beam-splitter then mixes modes 0 and 1, and the number of photons in each of

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

these modes is counted. The teleportation works whenever the total count on modes 0 and 1 is unity. To see this, it is instructive to consider what happens in the other cases. If the total count at the output is 0, then we can infer that initially mode $a_0$ must have been in the vacuum state. Likewise, if the total count is 2 then we can infer that initially mode $a_0$ must have contained a single photon. In both cases the output photon count serves to measure the number of photons in the input mode, destroying the quantum information there. This is a failure of the teleportation, but a so-called 'heralded' failure because we know it has occurred.

**Exercise 7.40** *Show that the probability of this heralded failure is* $1/2$*, independently of* $|\phi\rangle$*.*
**Hint:** *First show that, for this purpose, mode* $a_1$ *entering the second beam-splitter can be considered as being in either state* $|0\rangle$ *or state* $|1\rangle$*, each with probability* $1/2$*.*

If the teleporter does not fail as just described, then it succeeds. That is, the input state appears in mode 2 up to a simple transformation without having interacted with mode 2 after the preparation of the initial ancilla state.

**Exercise 7.41** *Taking the beam-splitter transformations to be*

$$|01\rangle \to \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \qquad |10\rangle \to \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle), \tag{7.130}$$

*show that the conditional states at mode* $a_2$ *when* $k + l = 1$ *are given by*

$$|\psi\rangle_2 = \begin{cases} \alpha|0\rangle_2 + \beta|1\rangle_2 & \text{for } k = 1, l = 0, \\ \alpha|0\rangle_2 - \beta|1\rangle_2 & \text{for } k = 0, l = 1. \end{cases} \tag{7.131}$$

In the second case, the state can be corrected back to $|\phi\rangle$ by applying the operator $Z$. In this single-rail case, this corresponds simply to an optical phase shift of $\pi$.

The probability of success of the above teleporter is 1/2, which is not acceptable. However, we can improve the probability of successful teleportation to $1 - 1/(n + 1)$ by generalizing the initial entangled resource from $|t_1\rangle_{12}$ to an $n$-photon state

$$|t_n\rangle_{1\cdots(2n)} = \sum_{j=0}^{n} |1\rangle^{\otimes j}|0\rangle^{\otimes(n-j)}|0\rangle^{\otimes j}|1\rangle^{\otimes(n-j)}/\sqrt{n+1}. \tag{7.132}$$

Here the notation $|a\rangle^{\otimes j}$ means $j$ copies of the state $|a\rangle$: $|a\rangle \otimes |a\rangle \otimes \cdots \otimes |a\rangle$. The modes are labelled 1 to $2n$, from left to right. Note that this could be thought of as a state of $2n$ single-rail qubits, or $n$ dual-rail qubits (with the $k$th qubit encoded in modes $n + k$ and $k$). States of this form can be prepared non-deterministically 'off-line' (i.e. prior to being needed in the quantum computation itself).

To teleport the state $\alpha|0\rangle_0 + \beta|1\rangle_0$ using $|t_n\rangle$, we first couple the modes 0 to $n$ by a unitary tranformation $\hat{F}_{n+1}$, which implements an $(n + 1)$-point Fourier transform on these

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

modes:

$$\hat{a}_k \to \frac{1}{\sqrt{n+1}} \sum_{l=0}^{n} \mathrm{e}^{\mathrm{i}2\pi kl/(n+1)} \hat{a}_l. \tag{7.133}$$

Since this is linear, it can be implemented with passive linear optics; for details see Ref. [KLM01]. After applying $\hat{F}_{n+1}$, we measure the number of photons in each of the modes 0 to $n$.

Suppose this measurement detects $k$ photons altogether. It is possible to show that, if $0 < k < n+1$, then the teleported state appears in mode $n+k$ and only needs to be corrected by applying a phase shift. The modes $2n-l$ are in state $|1\rangle$ for $0 \le l < (n-k)$ and can be reused in future preparations requiring single photons. The remaining modes are in the vacuum state $|0\rangle$. If $k=0$ the input state is measured and projected to $|0\rangle_0$, whereas if $k = n+1$ it is projected to $|1\rangle_0$. The probability of these two failure events is $1/(n+1)$, regardless of the input. Note that both the necessary correction and which mode we teleported to are unknown until after the measurement.

**Exercise 7.42** *Consider the above protocol for* $n = 3$. *Show that*

$$|t_2\rangle = \frac{1}{\sqrt{3}}(|0011\rangle + |1001\rangle + |1100\rangle). \tag{7.134}$$

*Say the results of photon counting on modes* 0, 1 *and* 2 *are* $r$, $s$ *and* $t$, *respectively. Show that the teleportation is successful iff* $0 < r+s+t < 3$. *Compute the nine distinct conditional states that occur in these instances and verify that success occurs with probability of* $2/3$.

The problem with the approach presented above is that, for large $n$, the obvious networks for preparing the required states have very low probabilities of success, but to attain the stringent accuracy requirements for quantum computing [NC00] one does require large $n$. However, it is possible to make use of the fact that failure is detected and corresponds to measurements in the photon-number basis. This allows exponential improvements in the probability of success for gates and state production with small $n$, using quantum codes and exploiting the properties of the failure behaviour of the non-deterministic teleportation. For details see Knill *et al.* [KLM01]. Franson [FDF$^+$02] suggested a scheme by which the probability of unsuccessfully teleporting the gate will scale as $1/n^2$ rather than $1/n$ for large $n$. Unfortunately the price is that gate failure does not simply result in an accidental qubit error, making it difficult to scale.

Some important improvements have been made to the original scheme, making quantum optical computing experimentally viable. Nielsen [Nie04] proposed a scheme based on the cluster-state model of quantum computation. This is an alternative name for the ‘one-way’ quantum computation introduced in Ref. [RB01], in which quantum measurement and control completely replace the unitary two-qubit gates of the conventional circuit model. A large entangled state (the ‘cluster’) is prepared, then measurements are performed on individual qubits, and the results are used to control single-qubit unitaries on other qubits in the cluster, which are then measured, and so on. The cluster state does not have to be completely constructed before the computation begins; to an extent it can be assembled on the fly, as described by Browne and Rudoplph [BR05]. This allows LOQC with far fewer physical resources than the original KLM scheme. The assembly of cluster states relies on the basic non-deterministic teleportation protocol introduced above, in which success is heralded. What makes these schemes viable is that failure corresponds to an accidental qubit measurement, as noted above, and the deleterious effect of this is restricted to a single locality within the growing cluster and can be repaired.

To conclude, we summarize the physical requirements for scalable linear optics quantum computation: (i) single-photon sources; (ii) fast, efficient single-photon detectors; (iii) low-loss linear optical networks; and (iv) fast electro-optical control. The specifications for the single-photon source are particularly challenging: it must produce a sequence of identical single-mode pulses containing exactly one photon. The key quality test is that it must be possible to demonstrate very high visibility in the interference of photons in successive pulses (known as Hong–Ou–Mandel interference [HOM87]). Potential single-photon sources have been demonstrated [MD04]. The requirement for fast single-photon detectors that can reliably distinguish zero, one and two photons is also difficult with current technology, but is achievable by a variety of means. Low photon loss is not in principle a problem, and there are LOQC protocols that can correct for loss [KLM01]. The required electro-optical control (which can be considered feedforward) is also not a problem in principle. However, it is certainly challenging because the slowness of electro-optics requires storing photons for microsecond time-scales. For small numbers of gates some of these technical requirements can be ignored, and there is a considerable body of experimental work in this area [KMN$^+$07, LZG$^+$07].

## 7.9 Adaptive phase measurement and single-rail LOQC

In Section 7.8.2 we introduced the dual-rail encoding for LOQC in order to show how one- and two-qubit gates could be implemented. However, as noted in Section 7.8.3, the basic unit for two-qubit gates, namely the non-deterministic teleporter of Fig. 7.15, works on single-rail qubits. This suggests that it is worth considering using single-rail encoding, if one could work out a way to do single-qubit unitaries in the two-dimensional subspace spanned by the single-mode Fock states $|0\rangle$ and $|1\rangle$. This idea was first tried in Ref. [LR02], where non-deterministic single-rail single-qubit gates were constructed. However, these gates had low probability of success and, moreover, to obtain high fidelities required commensurately many resources. The resources used were coherent states and photon counting.

More recently, it was shown [RLW05] that, by adding an extra resource, namely dyne detection and the ability to do feedback, the resource consumption of single-rail logic could be dramatically reduced. Specifically, this allowed a *deterministic* protocol to prepare arbitrary single-rail qubits and to convert dual-rail qubits into single-rail qubits. Moreover, the reverse conversion can be done (albeit non-deterministically), thus allowing dual-rail single-qubit gates to be applied to single-rail qubits. The basic idea is to use feedback and

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

dyne measurement to create an *adaptive phase measurement* [Wis95], as was realized experimentally [AAS$^+$02]. Since this section ties together the idea of adaptive measurement, from Chapter 2, with continuous quantum measurement and feedback theory, from Chapters 4–6, to find an application in quantum information processing, it seems a fitting topic on which to end this book.

### 7.9.1 Dyne measurement on single-rail qubits

Consider a single optical mode within a high-quality cavity prepared in state $|\psi(0)\rangle$ at time $t = 0$. Say the cavity has only one output beam, giving rise to an intensity decay rate $\gamma$. Say also that this beam is subject to unit-efficiency dyne detection with the local oscillator having phase $\Phi(t)$ (for homodyne detection, this phase is time-independent). Then, working in the frame rotating at the optical frequency, the linear quantum trajectory describing the system evolution is (see Section 4.4.3)

$$\mathrm{d}|\bar{\psi}_J(t)\rangle = \left[-\tfrac{1}{2}\gamma\hat{a}^\dagger\hat{a}\,\mathrm{d}t + \sqrt{\gamma}\mathrm{e}^{-\mathrm{i}\Phi(t)}\hat{a}J(t)\mathrm{d}t\right]|\bar{\psi}_J(t)\rangle. \tag{7.135}$$

Here $J(t)$ is the dyne current, which is ostensibly white noise in order for $\langle\bar{\psi}_J(t)|\bar{\psi}_J(t)\rangle$ to be the appropriate weight for a particular trajectory (see Section 4.4.3).

Now say that the mode initially contains at most one photon: $|\psi(0)\rangle = c_0|0\rangle + c_1|1\rangle$. Then there is a simple analytical solution for the conditioned state:

$$|\bar{\psi}_J(t)\rangle = (c_0 + c_1R_t^*)|0\rangle + c_1\mathrm{e}^{-\gamma t/2}|1\rangle, \tag{7.136}$$

where $R_t$ is a functional of the dyne photocurrent record up to time $t$:

$$R_t = \int_0^t \mathrm{e}^{\mathrm{i}\Phi(s)}\mathrm{e}^{-\gamma s/2}\sqrt{\gamma}\,J(s)\mathrm{d}s. \tag{7.137}$$

**Exercise 7.43** *Show this.*

The measurement is complete at time $t = \infty$, and the probability of obtaining a particular measurement record $\mathbf{J} = \{J(s)\colon 0 \le s < \infty\}$ is

$$\wp(\mathbf{J}) = \langle\bar{\psi}_{\mathbf{J}}(t)|\bar{\psi}_{\mathbf{J}}(t)\rangle\wp_{\text{ost}}(\mathbf{J}). \tag{7.138}$$

Here $\wp_{\text{ost}}(\mathbf{J})$ is the ostensible probability of $\mathbf{J}$; that is, the distribution it would have if $J(t)\mathrm{d}t$ were equal to a Wiener increment $\mathrm{d}W(t)$. Now, from the above solution (7.136), $\wp(\mathbf{J})$ depends upon the system state only via the single complex functional $A = R_\infty$. That is, all of the information about the system in the complete dyne record $\mathbf{J}$ is contained in the complex number $A$. We can thus regard the dyne measurement in this case as a measurement yielding the result $A$, with probability distribution

$$\wp(A)\mathrm{d}^2A = |c_0 + c_1A^*|^2\wp_{\text{ost}}(A)\mathrm{d}^2A. \tag{7.139}$$

Here $\wp_{\rm ost}(A)$ is the distribution for $A$ implied by setting $J(t){\rm d}t = {\rm d}W(t)$. Thus, the measurement can be described by the POM

$$\hat{E}(A){\rm d}^2A = (|0\rangle + A|1\rangle)(\langle 0| + A^*\langle 1|)\wp_{\rm ost}(A){\rm d}^2A. \tag{7.140}$$

In the above the shape of the mode exiting from the cavity is a decaying exponential $u(t) = \gamma{\rm e}^{-\gamma t}$. The mode-shape $u(t)$ means, for example, that the mean photon number in the part of the output field emitted in the interval $[t, t+{\rm d}t)$ is $|c_1|^2u(t){\rm d}t$.

**Exercise 7.44** *Verify this using the methods of Section 4.7.6.*

We can generalize the above theory to dyne detection upon a mode with an arbitrary mode-shape $u(t)$, such that $u(t) \geq 0$ and $U(\infty) = 1$, where

$$U(t) = \int_0^t u(s){\rm d}s. \tag{7.141}$$

We do this by defining a time-dependent decay rate, $\gamma(t) = u(t)/[U(t) - 1]$. Then we can consider modes with finite duration $[0, T]$, in which case $U(T) = 1$. For a general mode-shape, Eq. (7.140) still holds, but with $A = R_T$ and

$$R_t = \int_0^t {\rm e}^{{\rm i}\Phi(s)}\sqrt{u(s)}\,J(s){\rm d}s. \tag{7.142}$$

**Exercise 7.45** *Show this by considering $\gamma(t)$ as defined above.*

### *7.9.2 Adaptive phase measurement on single-rail qubits*

For any time $t < T$ the measurement is *incomplete* in the sense defined in Section 1.4.2. Thus one can change the sort of information obtained about the system by *adapting* the measurement at times $0 < t < T$ (see Section 2.5.2). In the present context, the only parameter that can be controlled by a feedback loop is the local oscillator phase $\Phi(t)$. This allows adaptive dyne detection as discussed in Section 2.6. Indeed, here we consider the adaptive scheme introduced in Ref. [Wis95] which was realized in the experiment of Armen *et al.* [AAS+02]. This is to set

$$\Phi(t) = \arg R_t + \pi/2. \tag{7.143}$$

From Eq. (7.142), we can then write a differential equation for $R$ as

$${\rm d}R_t = {\rm i}\frac{R_t}{|R_t|}\sqrt{u(t)}\,J(t){\rm d}t. \tag{7.144}$$

Bearing in mind that $[J(t){\rm d}t]^2 = {\rm d}t$ (both ostensibly and actually), this has the solution

$$R_t = \sqrt{U(t)}{\rm e}^{{\rm i}\varphi(t)}, \tag{7.145}$$

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

where

$$\varphi(t) = \int_0^t \sqrt{\frac{u(s)}{U(s)}}\, J(s)\mathrm{d}s. \tag{7.146}$$

**Exercise 7.46** *Verify Eq. (7.145).*
**Hint:** *Consider first the SDE for $|R|^2$ and then that for $\varphi(t) = [1/(2\mathrm{i})]\ln(R_t/R_t^*)$.*

Now ostensibly $J(s)\mathrm{d}s = \mathrm{d}W(s)$, so $\varphi(t)$ is a Gaussian random variable with mean zero and variance

$$\int_0^t \frac{u(s)}{U(s)}\,\mathrm{d}s = \log\left(\frac{U(t)}{U(0)}\right). \tag{7.147}$$

But $U(0) = 0$ by definition, so ostensibly the variance of $\varphi(t)$ is infinite. That is, under this adaptive scheme $A = R_T$ describes a variable with a random phase and a modulus of unity. Since the modulus is deterministic, it can contain no information about the system. Thus, under this scheme, all of the information is contained in $\theta = \arg(A)$. Since this is ostensibly random, the POM for this measurement is, from Eq. (7.140),

$$\hat{E}(\theta)\mathrm{d}\theta = |\theta\rangle\langle\theta|\frac{\mathrm{d}\theta}{\pi}. \tag{7.148}$$

Here $|\theta\rangle = (|0\rangle + \mathrm{e}^{\mathrm{i}\theta}|1\rangle)/\sqrt{2}$ is a truncated phase state [PB97]. This is precisely Example 2 introduced in Section 1.2.5 to illustrate measurements for which the effect $\hat{E}(\theta)\mathrm{d}\theta$ is not a projector.

This adaptive dyne detection is useful for estimating the unknown phase of an optical pulse [Wis95, WK97, WK98, AAS$^+$02], but for LOQC we are interested only in its role in state preparation when the system mode is entangled with other modes. Say the total state is $|\Psi\rangle$. Then, from Eq. (7.148), the conditioned state of the other modes after the measurement yielding result $\theta$ is

$$\langle\theta|\Psi\rangle/\sqrt{\pi}, \tag{7.149}$$

where the squared norm of this state is equal to the probability density for obtaining this outcome. We now discuss applications of this result.

### *7.9.3 Preparing arbitrary single-rail qubit states*

A basic qubit operation is the preparation of superposition states. For dual-rail encoding in LOQC this is trivial to perform by making single-qubit gates act on a one-photon state, as described in Section 7.8.2. Arbitrary single-rail superposition states, $\alpha|0\rangle + \mathrm{e}^{-\mathrm{i}\phi}\sqrt{1-\alpha^2}|1\rangle$, with $\alpha$ and $\phi$ real numbers, are not so easy to produce. Previous suggestions for deterministic production of such states involved nonlinearities significantly larger than is currently feasible. Alternatively, non-deterministic techniques based on photon counting [PPB98, LR02] have been described and experimentally demonstrated [LM02], but these have low probabilities of success. A non-deterministic scheme based on

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

homodyne detection has also been demonstrated [BBL04], but has a vanishing probability of success for high-fidelity preparation. We now show that it is possible deterministically to produce an arbitrary single-rail state from a single-photon state using linear optics and adaptive phase measurements.

We begin by splitting a single photon into two modes at a beam-splitter with intensity reflectivity $\eta$, producing $|\Psi\rangle = \sqrt{\eta}|1\rangle|0\rangle + \sqrt{1-\eta}|0\rangle|1\rangle$. If we then carry out an adaptive phase measurement on the first mode we obtain a result $\theta$, which prepares the second mode in state

$$\sqrt{\eta}|0\rangle + \mathrm{e}^{-\mathrm{i}\theta}\sqrt{1-\eta}|1\rangle. \qquad (7.150)$$

**Exercise 7.47** *Verify this, and show that the result $\theta$ is completely random (actually random, not just ostensibly random).*

Now, by feedforward onto a phase modulator on the second mode, this random phase can be changed into any desired phase $\theta'$. Thus we can deterministically produce the arbitrary state

$$\sqrt{\eta}|0\rangle + e^{-\mathrm{i}\theta'}\sqrt{1-\eta}|1\rangle. \qquad (7.151)$$

### *7.9.4 Quantum gates using adaptive phase measurements*

We now have to show how to perform single-qubit unitaries on our single-rail qubits. Some of these are easy, such as the phase rotation used above. However, others, such as the Hadamard gate (which is essential for quantum computation) are more difficult. This is defined by the transformations $|0\rangle \to (|0\rangle + |1\rangle)/\sqrt{2}$ and $|1\rangle \to (|0\rangle - |1\rangle)/\sqrt{2}$. A Hadamard transformation plus arbitrary phase rotation will allow us to perform arbitrary single-qubit unitaries [LR02]. A non-deterministic Hadamard transformation for single-rail qubits based on photon counting was described in Ref. [LR02], but its success probability was very low. Here we show that a Hadamard transformation based on a combination of photon counting and adaptive phase measurements, whilst still non-deterministic, can have a much higher success probability.

The key observation is that a deterministic mapping of dual-rail encoding into single-rail encoding can be achieved using adaptive phase measurements. Consider the arbitrary dual-rail qubit $\alpha|01\rangle + \mathrm{e}^{-\mathrm{i}\phi}\sqrt{1-\alpha^2}|10\rangle$. Suppose an adaptive phase measurement is made on the second rail of the qubit, giving the result $\theta$. If a phase shift of $-\theta$ is subsequently imposed on the remaining rail of the qubit, the resulting state is $\alpha|0\rangle + \mathrm{e}^{-\mathrm{i}\phi}\sqrt{1-\alpha^2}|1\rangle$, which is a single-rail qubit with the same logical value as the original dual-rail qubit.

What about the reverse operation from a single-rail encoded qubit to a dual-rail encoded qubit? It does not appear to be possible to do this deterministically with only linear optics. However, a non-deterministic transformation is possible by teleporting between encodings. Dual-rail teleportation can be achieved using a dual-rail Bell state such as $|01\rangle|10\rangle + |10\rangle|01\rangle$. (We are ignoring normalization for convenience.) Single-rail teleportation can be

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

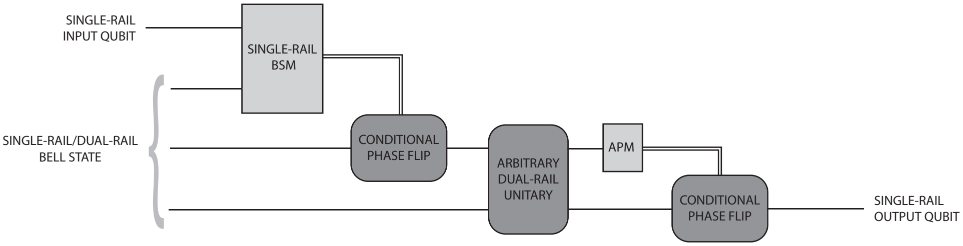

Fig. 7.16 A schematic representation of the application of an arbitrary single-qubit unitary to a single-rail qubit. The single-rail qubit is teleported onto a dual-rail qubit, the unitary is applied, then an adaptive phase measurement is used to convert back to a single-rail qubit. BSM means Bell-state measurement and APM means adaptive phase measurement. All operations are deterministic except the Bell-state measurement, which succeeds 50% of the time. Based on Figure 1 from T. C. Ralph *et al.*, Adaptive Phase Measurements in Linear Optical Quantum Computation, *Journal of Optics* B **7**, S245, (2005), IOP Publishing Ltd.

achieved using a single-rail Bell state such as $|0\rangle|1\rangle + |1\rangle|0\rangle$. In both cases only two of the four Bell states can be identified with linear optics, so the teleportation works 50% of the time, as illustrated in Fig. 7.16.

Now suppose we take a dual-rail Bell state and use an adaptive phase measurement to project one of its arms into a single-rail state. We obtain the state $|0\rangle|10\rangle + |1\rangle|01\rangle$, which is Bell entanglement between dual- and single-rail qubits. If we now perform a Bell measurement between the single-rail half of the entanglement and an arbitrary single-rail qubit then (when successful) the qubit will be teleported onto the dual-rail part of the entanglement, thus converting a single-rail qubit into a dual-rail qubit.

We now have a way of (non-deterministically) performing an arbitrary rotation on an unknown single-rail qubit. The idea is depicted schematically in Fig. 7.16. First we teleport the single-rail qubit onto a dual-rail qubit. Then we perform an arbitrary rotation on the dual-rail qubit. We then use an adaptive phase measurement to transform the dual-rail qubit back into a single-rail qubit. The only non-deterministic step is the Bell measurement in the teleportation, which in this simple scheme has a success probability of 50%. This is a major improvement over previous schemes. As discussed in Section 7.8.3, the success probability for this step can be increased arbitrarily by using larger entangled resources. Also as discussed in that section, the fundamental two-qubit gate, the CS gate, is in fact a single-rail gate. Thus, by employing quantum feedback control we are able to perform universal quantum computation in LOQC using single-rail encoding.

## 7.10 Further reading

There are many other applications of measurement and control in quantum information processing besides those mentioned in this chapter. Here are a few of them.

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

*Rapid purification of a qubit.* A two-level quantum system initially in a completely mixed state will gradually purify to a $\hat{\sigma}_z$ eigenstate under a continuous QND measurement of $\hat{\sigma}_z$ (as in Eq. (5.204) of Section 5.7, but for a single spin). It was shown by Jacobs [Jac03] that, using feedback control to make the state always unbiased with respect to $\hat{\sigma}_z$ (that is, to keep the system Bloch vector in the $x$–$y$ plane), the information gain from the QND measurement is greater. That is, the rate of increase of the *average purity* of the system can be increased. Moreover, this is achieved by Markovian feedback of the QND current with a time-varying feedback strength, as in Section 5.7. In the asymptotic limit of high purity (long times) the system can be purified to any given degree using measurement and feedback in half the time it would take from the measurement alone. Note, however, that different results are obtained from considering the *average time* required to obtain a given level of purity – see Refs. [WR06, CWJ08, WB08].

*Mitigating the effect of a noisy channel.* Consider a qubit prepared in one of two non-orthogonal states in the $x$–$z$ plane of the Bloch sphere, with the same value of $x$ but opposite values of $z$. Say this qubit is subjected to dephasing noise; that is, a rotation around the $z$ axis by a random angle described by some probability distribution. The task is to use measurement and feedback control to attempt to correct the state of the qubit; that is, to undo the effect of the *noisy channel*. It was demonstrated in Ref. [BMG$^+$07] that projective measurements are not optimal for this task and that there exists a non-projective measurement with an optimum measurement strength that achieves the best trade-off between gaining information about the system (or the noise) and disturbing it through measurement back-action. Moreover, a quantum control scheme that makes use of this weak measurement followed by feedback control is provably optimal for ameliorating the effect of noise on this system.

*Controlling decoherence by dynamical decoupling.* In this chapter we have discussed methods of controlling decoherence that are based on quantum error correction, both for undetected errors (conventional quantum error correction) and for detected errors. An alternative is to try to prevent the errors from happening in the first place by decoupling the system from its environment. *Dynamical decoupling*, introduced by Viola and co-workers [VLK99], uses open-loop control, without ancillae or measurement. On the basis of the idea of bang-bang control [VL98], the quantum system is subjected to a sequence of impulsive unitary transformations so that the evolution is described on longer time-scales by an effective modified Hamiltonian in which unwanted interactions are suppressed. In later work [SV06] the idea of a randomly generated (but known to the experimenter) sequence of unitary control pulses was shown to overcome some of the limitations for regular dynamical decoupling when there are rapidly fluctuating interactions or when the usual deterministically generated sequence of control pulses would be too long to implement.

*Adaptive phase estimation inspired by quantum computing.* At the heart of Shor's 1994 factoring algorithm is a routine known as the quantum phase-estimation algorithm [NC00]. It relates to accurately estimating the eigenvalues of an unknown unitary operator and involves an algorithm called the quantum Fourier transform (QFT). As shown in Ref. [GN96], the QFT algorithm can be performed using single-qubit measurement

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press

and control, much as in cluster-state quantum computing as discussed above. In fact, the quantum phase-estimation algorithm can be used as an (adaptive) protocol for estimating the phase $\phi$ in a single-qubit phase gate $\exp(i\phi Z/2)$, using *only* single-qubit operations (preparations, measurements and control), as long as it is possible for the gate to be applied multiple times to a given single qubit between preparation and measurement [GLM06]. The quantum phase-estimation algorithm enables a canonical measurement of phase (see Section 2.4), but the nature of the prepared states means that it does not attain the Heisenberg limit for the phase variance (2.133). However, a simple generalization of the quantum phase-estimation algorithm, using the principles of adaptive phase estimation discussed in Section 2.5, enables a variance scaling at the Heisenberg limit to be achieved, with an overhead factor of less than 2.5 [HBB$^+$07]. Moreover, this was recently demonstrated experimentally by Higgins *et al.* using single-photon multi-pass interferometry [HBB$^+$07] – the first experiment to demonstrate Heisenberg-limited scaling for phase estimation. In this chapter, we have concentrated on showing that quantum computing can benefit from an understanding of quantum measurement and control, but this work demonstrates that the converse is also true.

https://doi.org/10.1017/CBO9780511813948.008 Published online by Cambridge University Press