putation. This is made possible by completing the computation in time short compared with the measurement coupling, and by using large ensembles of quantum computers. These ensembles together give an aggregate signal which is macroscopically observable and indicative of the quantum state. Use of an ensemble introduces additional problems. For example, in the factoring algorithm, if the measurement output is $q\langle c\rangle/r$, the algorithm would fail because $\langle c\rangle$, the average value of c, is not necessarily an integer (and thus the continued fraction expansion would not be possible). Fortunately, it is possible to modify quantum algorithms to work with ensemble average readouts. This will be discussed further in Section 7.7.

A good figure of merit for measurement capability is the signal to noise ratio (SNR). This accounts for measurement inefficiency as well as inherent signal strength available from coupling a measurement apparatus to the quantum system.

7.3 Harmonic oscillator quantum computer

Before continuing on to describe a complete physical model for a realizable quantum computer, let us pause for a moment to consider a very elementary system – the simple harmonic oscillator – and discuss why it does not serve as a good quantum computer. The formalism used in this example will also serve as a basis for studying other physical systems.

7.3.1 Physical apparatus

An example of a simple harmonic oscillator is a particle in a parabolic potential well, $V(x) = m\omega^2 x^2/2$. In the classical world, this could be a mass on a spring, which oscillates back and forth as energy is transfered between the potential energy of the spring and the kinetic energy of the mass. It could also be a resonant electrical circuit, where the energy sloshes back and forth between the inductor and the capacitor. In these systems, the total energy of the system is a continuous parameter.

In the quantum domain, which is reached when the coupling to the external world becomes very small, the total energy of the system can only take on a discrete set of values. An example is given by a single mode of electromagnetic radiation trapped in a high Q cavity; the total amount of energy (up to a fixed offset) can only be integer multiples of $\hbar\omega$, an energy scale which is determined by the fundamental constant $\hbar$ and the frequency of the trapped radiation, ω.

The set of discrete energy eigenstates of a simple harmonic oscillator can be labeled as $|n\rangle$, where $n = 0, 1, \ldots, \infty$. The relationship to quantum computation comes by taking a finite subset of these states to represent qubits. These qubits will have lifetimes determined by physical parameters such as the cavity quality factor Q, which can be made very large by increasing the reflectivity of the cavity walls. Moreover, unitary transforms can be applied by simply allowing the system to evolve in time. However, there are problems with this scheme, as will become clear below. We begin by studying the system Hamiltonian, then discuss how one might implement simple quantum logic gates such as the controlled-NOT.

7.3.2 The Hamiltonian

The Hamiltonian for a particle in a one-dimensional parabolic potential is

$$H = \frac{p^2}{2m} + \frac{1}{2}m\omega^2 x^2 \,, \tag{7.4}$$

where p is the particle momentum operator, m is the mass, x is the position operator, and ω is related to the potential depth. Recall that x and p are operators in this expression (see Box 7.2), which can be rewritten as

$$H = \hbar\omega\left(a^\dagger a + \frac{1}{2}\right) \,, \tag{7.5}$$

where $a^\dagger$ and a are creation and annihilation operators, defined as

$$a = \frac{1}{\sqrt{2m\hbar\omega}}\left(m\omega x + ip\right) \tag{7.6}$$

$$a^\dagger = \frac{1}{\sqrt{2m\hbar\omega}}\left(m\omega x - ip\right) \,. \tag{7.7}$$

The zero point energy $\hbar\omega/2$ contributes an unobservable overall phase factor, which can be disregarded for our present purpose.

The eigenstates $|n\rangle$ of H, where $n = 0, 1, \ldots$, have the properties

$$a^\dagger a|n\rangle = n|n\rangle \tag{7.10}$$

$$a^\dagger|n\rangle = \sqrt{n+1}\,|n+1\rangle \tag{7.11}$$

$$a|n\rangle = \sqrt{n}\,|n-1\rangle \,. \tag{7.12}$$

Later, we will find it convenient to express interactions with a simple harmonic oscillator by introducing additional terms involving a and $a^\dagger$, and interactions between oscillators with terms such as $a_1^\dagger a_2 + a_1 a_2^\dagger$. For now, however, we confine our attention to a single oscillator.

Exercise 7.1: Using the fact that x and p do not commute, and that in fact $[x, p] = i\hbar$, explicitly show that $a^\dagger a = H/\hbar\omega - 1/2$.

Exercise 7.2: Given that $[x, p] = i\hbar$, compute $[a, a^\dagger]$.

Exercise 7.3: Compute $[H, a]$ and use the result to show that if $|\psi\rangle$ is an eigenstate of H with energy $E \geq n\hbar\omega$, then $a^n|\psi\rangle$ is an eigenstate with energy $E - n\hbar\omega$.

Exercise 7.4: Show that $|n\rangle = \frac{(a^\dagger)^n}{\sqrt{n!}}|0\rangle$.

Exercise 7.5: Verify that Equations (7.11) and (7.12) are consistent with (7.10) and the normalization condition $\langle n|n\rangle = 1$.

Time evolution of the eigenstates is given by solving the Schrödinger equation, (2.86), from which we find that the state $|\psi(0)\rangle = \sum_n c_n(0)|n\rangle$ evolves in time to become

$$|\psi(t)\rangle = e^{-iHt/\hbar}|\psi(0)\rangle = \sum_n c_n e^{-in\omega t}|n\rangle \,. \tag{7.13}$$

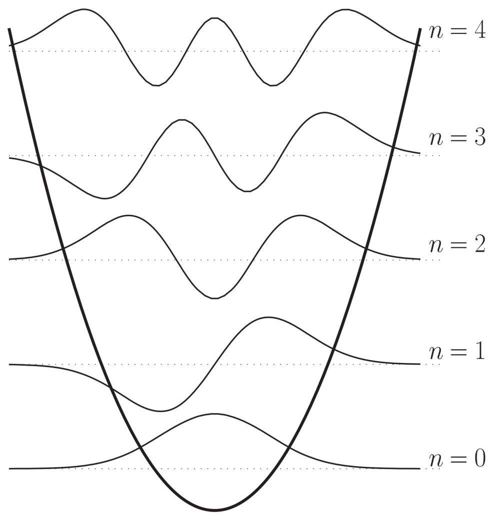
We will assume for the purpose of discussion that an arbitrary state can be perfectly prepared, and that the state of the system can be projectively measured (Section 2.2.3),

Box 7.2: The quantum harmonic oscillator

The harmonic oscillator is an extremely important and useful concept in the quantum description of the physical world, and a good way to begin to understand its properties is to determine the energy eigenstates of its Hamiltonian, (7.4). One way to do this is simply to solve the Schrödinger equation

$$\frac{\hbar^2}{2m}\frac{d^2\psi_n(x)}{dx^2} + \frac{1}{2}m\omega^2 x^2\psi_n(x) = E\psi_n(x) \tag{7.8}$$

for $\psi_n(x)$ and the eigenenergies E, subject to $\psi(x) \to 0$ at $x = \pm\infty$, and $\int |\psi(x)|^2 = 1$; the first five solutions are sketched here:



These wavefunctions describe the probability amplitudes that a particle in the harmonic oscillator will be found at different positions within the potential.

Although these pictures may give some intuition about what a physical system is doing in co-ordinate space, we will generally be more interested in the abstract *algebraic* properties of the states. Specifically, suppose $|\psi\rangle$ satisfies (7.8) with energy E. Then defining operators a and $a^\dagger$ as in (7.6)–(7.7), we find that since $[H, a^\dagger] = \hbar\omega a^\dagger$,

$$Ha^\dagger|\psi\rangle = \Big([H, a^\dagger] + a^\dagger H\Big)|\psi\rangle = (\hbar\omega + E)a^\dagger|\psi\rangle\,, \tag{7.9}$$

that is, $a^\dagger|\psi\rangle$ is an eigenstate of H, with energy $E + \hbar\omega$! Similarly, $a|\psi\rangle$ is an eigenstate with energy $E - \hbar\omega$. Because of this, $a^\dagger$ and a are called raising and lowering operators. It follows that ${a^\dagger}^n|\psi\rangle$ are eigenstates for any integer n, with energies $E + n\hbar\omega$. There are thus an infinite number of energy eigenstates, whose energies are equally spaced apart, by $\hbar\omega$. Moreover, since H is positive definite, there must be some $|\psi_0\rangle$ for which $a|\psi_0\rangle = 0$; this is the ground state – the eigenstate of H with lowest energy. These results efficiently capture the essence of the quantum harmonic oscillator, and allow us to use a compact notation $|n\rangle$ for the eigenstates, where n is an integer, and $H|n\rangle = \hbar(n + 1/2)|n\rangle$. We shall often work with $|n\rangle$, a, and $a^\dagger$ in this chapter, as harmonic oscillators arise in the guise of many different physical systems.

but otherwise, there are no interactions with the external world, so that the system is perfectly closed.

7.3.3 Quantum computation

Suppose we want to perform quantum computation with the single simple harmonic oscillator described above. What can be done? The most natural choice for representation of qubits are the energy eigenstates $|n\rangle$. This choice allows us to perform a controlled-NOT gate in the following way. Recall that this transformation performs the mapping

$$\begin{array}{ccc} |00\rangle_L & \to & |00\rangle_L \\ |01\rangle_L & \to & |01\rangle_L \\ |10\rangle_L & \to & |11\rangle_L \\ |11\rangle_L & \to & |10\rangle_L \,, \end{array} \tag{7.14}$$

on two qubit states (here, the subscript L is used to clearly distinguish 'logical' states in contrast to the harmonic oscillator basis states). Let us *encode* these two qubits using the mapping

$$\begin{array}{ccl} |00\rangle_L & = & |0\rangle \\ |01\rangle_L & = & |2\rangle \\ |10\rangle_L & = & (|4\rangle + |1\rangle)/\sqrt{2} \\ |11\rangle_L & = & (|4\rangle - |1\rangle)/\sqrt{2}\,. \end{array} \tag{7.15}$$

Now suppose that at $t = 0$ the system is started in a state spanned by these basis states, and we simply evolve the system forward to time $t = \pi/\hbar\omega$. This causes the energy eigenstates to undergo the transformation $|n\rangle \to \exp(-i\pi a^\dagger a)|n\rangle = (-1)^n|n\rangle$, such that $|0\rangle$, $|2\rangle$, and $|4\rangle$ stay unchanged, but $|1\rangle \to -|1\rangle$. As a result, we obtain the desired controlled-NOT gate transformation.

In general, a necessary and sufficient condition for a physical system to be able to perform a unitary transform U is simply that the time evolution operator for the system, $T = \exp(-iHt)$, defined by its Hamiltonian H, has nearly the same eigenvalue spectrum as U. In the case above, the controlled-NOT gate was simple to implement because it only has eigenvalues $+1$ and -1; it was straightforward to arrange an encoding to obtain the same eigenvalues from the time evolution operator for the harmonic oscillator. The Hamiltonian for an oscillator could be perturbed to realize nearly any eigenvalue spectrum, and any number of qubits could be represented by simply mapping them into the infinite number of eigenstates of the system. This suggests that perhaps one might be able to realize an entire quantum computer in a single simple harmonic oscillator!

7.3.4 Drawbacks

Of course, there are many problems with the above scenario. Clearly, one will not always know the eigenvalue spectrum of the unitary operator for a certain quantum computation, even though one may know how to construct the operator from elementary gates. In fact, for most problems addressed by quantum algorithms, knowledge of the eigenvalue spectrum is tantamount to knowledge of the solution!

Another obvious problem is that the technique used above does not allow one computation to be cascaded with another, because in general, cascading two unitary transforms results in a new transform with unrelated eigenvalues.

Finally, the idea of using a single harmonic oscillator to perform quantum computation is flawed because it neglects the principle of digital representation of information. A Hilbert space of 2^n dimensions mapped into the state space of a single harmonic oscillator would have to allow for the possibility of states with energy $2^n\hbar\omega$. In contrast, the same Hilbert space could be obtained by using n two-level quantum systems, which has an energy of at most $n\hbar\omega$. Similar comparisons can be made between a classical dial with 2^n settings, and a register of n classical bits. Quantum computation builds upon *digital* computation, not analog computation.

The main features of the harmonic oscillator quantum computer are summarized below (each system we consider will be summarized similarly, at the end of the corresponding section). With this, we leave behind us the study of single oscillators, and turn next to systems of harmonic oscillators, made of photons and atoms.

Harmonic oscillator quantum computer

- **Qubit representation**: Energy levels $|0\rangle, |1\rangle, \ldots, |2^n\rangle$ of a single quantum oscillator give n qubits.
- **Unitary evolution**: Arbitrary transforms U are realized by matching their eigenvalue spectrums to that given by the Hamiltonian $H = a^\dagger a$.
- **Initial state preparation**: Not considered.
- **Readout**: Not considered.
- **Drawbacks**: Not a digital representation! Also, matching eigenvalues to realize transformations is not feasible for arbitrary U, which generally have unknown eigenvalues.

7.4 Optical photon quantum computer

An attractive physical system for representing a quantum bit is the optical photon. Photons are chargeless particles, and do not interact very strongly with each other, or even with most matter. They can be guided along long distances with low loss in optical fibers, delayed efficiently using phase shifters, and combined easily using beamsplitters. Photons exhibit signature quantum phenomena, such as the interference produced in two-slit experiments. Furthermore, in principle, photons *can* be made to interact with each other, using nonlinear optical media which mediate interactions. There are problems with this ideal scenario; nevertheless, many things can be learned from studying the components, architecture, and drawbacks of an optical photon quantum information processor, as we shall see in this section.

7.4.1 Physical apparatus

Let us begin by considering what single photons are, how they can represent quantum states, and the experimental components useful for manipulating photons. The classical behavior of phase shifters, beamsplitters, and nonlinear optical Kerr media is described.

Photons can represent qubits in the following manner. As we saw in the discussion of the simple harmonic oscillator, the energy in an electromagnetic cavity is quantized in units of $\hbar\omega$. Each such quantum is called a photon. It is possible for a cavity to contain a superposition of zero or one photon, a state which could be expressed as a qubit $c_0|0\rangle + c_1|1\rangle$, but we shall do something different. Let us consider two cavities, whose total energy is $\hbar\omega$, and take the two states of a qubit as being whether the photon is in one cavity ($|01\rangle$) or the other ($|10\rangle$). The physical state of a superposition would thus be written as $c_0|01\rangle + c_1|10\rangle$; we shall call this the *dual-rail* representation. Note that we shall focus on single photons traveling as a wavepacket through free space, rather than inside a cavity; one can imagine this as having a cavity moving along with the wavepacket. Each cavity in our qubit state will thus correspond to a different spatial mode.

One scheme for generating single photons in the laboratory is by attenuating the output of a laser. A laser outputs a state known as a coherent state, $|\alpha\rangle$, defined as

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,, \tag{7.16}$$

where $|n\rangle$ is an n-photon energy eigenstate. This state, which has been the subject of thorough study in the field of quantum optics, has many beautiful properties which we shall not describe here. It suffices to understand just that coherent states are naturally radiated from driven oscillators such as a laser when pumped high above its lasing threshold. Note that the mean energy is $\langle\alpha|n|\alpha\rangle = |\alpha|^2$. When attenuated, a coherent state just becomes a weaker coherent state, and a weak coherent state can be made to have just one photon, with high probability.

Exercise 7.6: (Eigenstates of photon annihilation) Prove that a coherent state is an eigenstate of the photon annihilation operator, that is, show $a|\alpha\rangle = \lambda|\alpha\rangle$ for some constant λ.

For example, for $\alpha = \sqrt{0.1}$, we obtain the state $\sqrt{0.90}\,|0\rangle + \sqrt{0.09}\,|1\rangle + \sqrt{0.002}\,|2\rangle + \cdots$. Thus if light ever makes it through the attenuator, one knows it is a single photon with probability better than 95%; the failure probability is thus 5%. Note also that 90% of the time, no photons come through at all; this source thus has a rate of 0.1 photons per unit time. Finally, this source does not indicate (by means of some classical readout) when a photon has been output or not; two of these sources cannot be synchronized.

Better synchronicity can be achieved using parametric down-conversion. This involves sending photons of frequency ω_0 into a nonlinear optical medium such as KH_2PO_4 to generate photon pairs at frequencies $\omega_1 + \omega_2 = \omega_0$. Momentum is also conserved, such that $\vec{k}_1 + \vec{k}_2 = \vec{k}_3$, so that when a single ω_2 photon is (destructively) detected, then a single ω_1 photon is known to exist (Figure 7.2). By coupling this to a gate, which is opened only when a single photon (as opposed to two or more) is detected, and by appropriately delaying the outputs of multiple down-conversion sources, one can, in principle, obtain multiple single photons propagating in time synchronously, within the time resolution of the detector and gate.

Single photons can be detected with high quantum efficiency for a wide range of wavelengths, using a variety of technologies. For our purposes, the most important characteristic of a detector is its capability of determining, with high probability, whether zero or one photon exists in a particular spatial mode. For the dual-rail representation, this translates into a projective measurement in the computational basis. In practice, imperfections reduce the probability of being able to detect a single photon; the *quantum efficiency* η $(0 \leq \eta \leq 1)$ of a photodetector is the probability that a single photon incident on the detector generates a photocarrier pair that contributes to detector current. Other important characteristics of a detector are its bandwidth (time responsivity), noise, and 'dark counts' which are photocarriers generated even when no photons are incident.

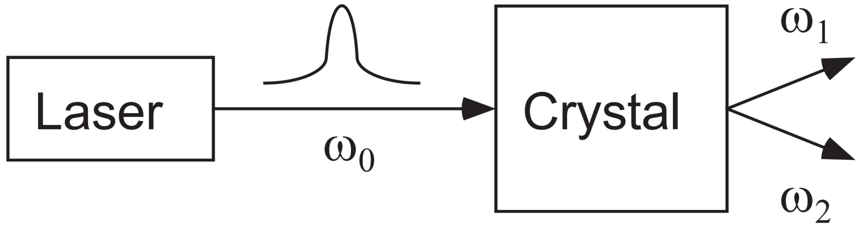


Figure 7.2. Parametric down-conversion scheme for generation of single photons.

Three of the most experimentally accessible devices for manipulating photon states are mirrors, phase shifters and beamsplitters. High reflectivity mirrors reflect photons and change their propagation direction in space. Mirrors with 0.01% loss are not unusual. We shall take these for granted in our scenario. A phase shifter is nothing more than a slab of transparent medium with index of refraction n different from that of free space, n_0; for example, ordinary borosilicate glass has $n \approx 1.5n_0$ at optical wavelengths. Propagation in such a medium through a distance L changes a photon's phase by e^{ikL}, where $k = n\omega/c_0$, and c_0 is the speed of light in vacuum. Thus, a photon propagating through a phase shifter will experience a phase shift of $e^{i(n-n_0)L\omega/c_0}$ compared to a photon going the same distance through free space.

Another useful component, the beamsplitter, is nothing more than a partially silvered piece of glass, which reflects a fraction R of the incident light, and transmits $1-R$. In the laboratory, a beamsplitter is usually fabricated from two prisms, with a thin metallic layer sandwiched in-between, schematically drawn as shown in Figure 7.3. It is convenient to define the *angle* θ of a beamsplitter as $\cos\theta = R$; note that the angle parameterizes the amount of partial reflection, and does not necessarily have anything to do with the physical orientation of the beamsplitter. The two inputs and two outputs of this device are related by

$$a_{out} = a_{in}\cos\theta + b_{in}\sin\theta \tag{7.17}$$

$$b_{out} = -a_{in}\sin\theta + b_{in}\cos\theta\,, \tag{7.18}$$

where classically we think of a and b as being the electromagnetic fields of the radiation at the two ports. Note that in this definition we have chosen a non-standard phase convention convenient for our purposes. In the special case of a 50/50 beamsplitter, $\theta = 45°$.

Nonlinear optics provides one final useful component for this exercise: a material

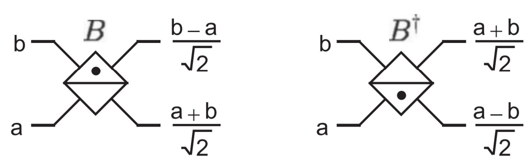


Figure 7.3. Schematic of an optical beamsplitter, showing the two input ports, the two output ports, and the phase conventions for a 50/50 beamsplitter ($\theta = \pi/4$). The beamsplitter on the right is the inverse of the one on the left (the two are distinguished by the dot drawn inside). The input-output relations for the mode operators a and b are given for $\theta = \pi/4$.

whose index of refraction n is proportional to the total intensity I of light going through it:

$$n(I) = n + n_2 I \,. \tag{7.19}$$

This is known as the optical Kerr effect, and it occurs (very weakly) in materials as mundane as glass and sugar water. In doped glasses, n_2 ranges from 10^{-14} to 10^{-7} cm^2/W, and in semiconductors, from 10^{-10} to 10^2. Experimentally, the relevant behavior is that when two beams of light of equal intensity are nearly co-propagated through a Kerr medium, each beam will experience an extra phase shift of $e^{in_2 IL\omega/c_0}$ compared to what happens in the single beam case. This would be ideal if the length L could be arbitrarily long, but unfortunately that fails because most Kerr media are also highly absorptive, or scatter light out of the desired spatial mode. This is the primary reason why a single photon quantum computer is impractical, as we shall discuss in Section 7.4.3.

We turn next to a quantum description of these optical components.

7.4.2 Quantum computation

Arbitrary unitary transforms can be applied to quantum information, encoded with single photons in the $c_0|01\rangle + c_1|10\rangle$ dual-rail representation, using phase shifters, beamsplitters, and nonlinear optical Kerr media. How this works can be understood in the following manner, by giving a quantum-mechanical Hamiltonian description of each of these devices.

The time evolution of a cavity mode of electromagnetic radiation is modeled quantum-mechanically by a harmonic oscillator, as we saw in Section 7.3.2. $|0\rangle$ is the vacuum state, $|1\rangle = a^\dagger|0\rangle$ is a single photon state, and in general, $|n\rangle = \frac{a^{\dagger n}}{\sqrt{n!}}|0\rangle$ is an n-photon state, where $a^\dagger$ is the creation operator for the mode. Free space evolution is described by the Hamiltonian

$$H = \hbar\omega a^\dagger a \,, \tag{7.20}$$

and applying (7.13), we find that the state $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ evolves in time to become $|\psi(t)\rangle = c_0|0\rangle + c_1 e^{-i\omega t}|1\rangle$. Note that the dual-rail representation is convenient because free evolution only changes $|\varphi\rangle = c_0|01\rangle + c_1|10\rangle$ by an overall phase, which is undetectable. Thus, for that manifold of states, the evolution Hamiltonian is zero.

Phase shifter. A phase shifter P acts just like normal time evolution, but at a different rate, and localized to only the modes going through it. That is because light slows down in a medium with larger index of refraction; specifically, it takes $\Delta \equiv (n - n_0)L/c_0$ more time to propagate a distance L in a medium with index of refraction n than in vacuum. For example, the action of P on the vacuum state is to do nothing: $P|0\rangle = |0\rangle$, but on a single photon state, one obtains $P|1\rangle = e^{i\Delta}|1\rangle$.

P performs a useful logical operation on a dual-rail state. Placing a phase shifter in one mode retards its phase evolution with respect to another mode, which travels the same distance but without going through the shifter. For dual-rail states this transforms $c_0|01\rangle + c_1|10\rangle$ to $c_0 e^{-i\Delta/2}|01\rangle + c_1 e^{i\Delta/2}|10\rangle$, up to an irrelevant overall phase. Recall from Section 4.2 that this operation is nothing more than a rotation,

$$R_z(\Delta) = e^{-iZ\Delta/2} \,, \tag{7.21}$$

where we take as the logical zero $|0_L\rangle = |01\rangle$ and one $|1_L\rangle = |10\rangle$, and Z is the usual

Pauli operator. One can thus think of P as resulting from time evolution under the Hamiltonian

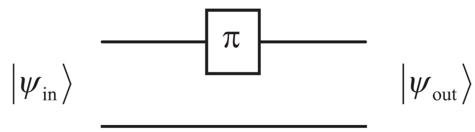
$$H = (n_0 - n)Z\,, \tag{7.22}$$

where $P = \exp(-iHL/c_0)$.

Exercise 7.7: Show that the circuit below transforms a dual-rail state by

$$|\psi_{out}\rangle = \begin{bmatrix} e^{i\pi} & 0 \\ 0 & 1 \end{bmatrix} |\psi_{in}\rangle\,, \tag{7.23}$$

if we take the top wire to represent the $|01\rangle$ mode, and $|10\rangle$ the bottom mode, and the boxed π to represent a phase shift by π:



Note that in such 'optical circuits', propagation in space is explicitly represented by putting in lumped circuit elements such as in the above, to represent phase evolution. In the dual-rail representation, evolution according to (7.20) changes the logical state only by an unobservable global phase, and thus we are free to disregard it and keep only relative phase shifts.

Exercise 7.8: Show that $P|\alpha\rangle = |\alpha e^{i\Delta}\rangle$ where $|\alpha\rangle$ is a coherent state (note that, in general, α is a complex number!).

Beamsplitter. A similar Hamiltonian description of the beamsplitter also exists, but instead of motivating it phenomenologically, let us begin with the Hamiltonian and show how the expected classical behavior, Equations (7.17)–(7.18) arises from it. Recall that the beamsplitter acts on two modes, which we shall describe by the creation (annihilation) operators a ($a^\dagger$) and b ($b^\dagger$). The Hamiltonian is

$$H_{bs} = i\theta\left(ab^\dagger - a^\dagger b\right)\,, \tag{7.24}$$

and the beamsplitter performs the unitary operation

$$B = \exp\left[\theta\left(a^\dagger b - ab^\dagger\right)\right]\,. \tag{7.25}$$

The transformations effected by B on a and b, which will later be useful, are found to be

$$BaB^\dagger = a\cos\theta + b\sin\theta \qquad \text{and} \qquad BbB^\dagger = -a\sin\theta + b\cos\theta\,. \tag{7.26}$$

We verify these relations using the Baker–Campbell–Hausdorf formula (also see Exercise 4.49)

$$e^{\lambda G} A e^{-\lambda G} = \sum_{n=0}^{\infty} \frac{\lambda^n}{n!} C_n\,, \tag{7.27}$$

where λ is a complex number, A, G, and C_n are operators, and C_n is defined recursively as the sequence of commutators $C_0 = A$, $C_1 = [G, C_0]$, $C_2 = [G, C_1]$, $C_3 = [G, C_2]$, ..., $C_n = [G, C_{n-1}]$. Since it follows from $[a, a^\dagger] = 1$ and $[b, b^\dagger] = 1$ that $[G, a] = -b$ and $[G, b] = a$, for $G \equiv a^\dagger b - ab^\dagger$, we obtain for the expansion of $BaB^\dagger$ the series coefficients

$C_0 = a$, $C_1 = [G, a] = -b$, $C_2 = [G, C_1] = -a$, $C_3 = [G, C_2] = -[G, C_0] = b$, which in general are

$$C_{n \text{ even}} = i^n a \tag{7.28}$$
$$C_{n \text{ odd}} = i^{n+1} b\,. \tag{7.29}$$

From this, our desired result follows straightforwardly:

$$BaB^\dagger = e^{\theta G} a e^{-\theta G} \tag{7.30}$$
$$= \sum_{n=0}^{\infty} \frac{\theta^n}{n!} C_n \tag{7.31}$$
$$= \sum_{n \text{ even}} \frac{(i\theta)^n}{n!} a + i \sum_{n \text{ odd}} \frac{(i\theta)^n}{n!} b \tag{7.32}$$
$$= a \cos\theta - b \sin\theta\,. \tag{7.33}$$

The transform $BbB^\dagger$ is trivially found by swapping a and b in the above solution. Note that the beamsplitter operator arises from a deep relationship between the beamsplitter and the algebra of $SU(2)$, as explained in Box 7.3.

In terms of quantum logic gates, B performs a useful operation. First note that $B|00\rangle = |00\rangle$, that is, when no photons in either input mode exist, no photons will exist in either output mode. When one photon exists in mode a, recalling that $|1\rangle = a^\dagger|0\rangle$, we find that

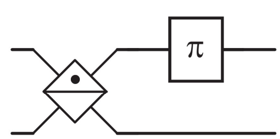
$$B|01\rangle = Ba^\dagger|00\rangle = Ba^\dagger B^\dagger B|00\rangle = (a^\dagger \cos\theta + b^\dagger \sin\theta)|00\rangle = \cos\theta|01\rangle + \sin\theta|10\rangle\,. \tag{7.34}$$

Similarly, $B|10\rangle = \cos\theta|10\rangle - \sin\theta|01\rangle$. Thus, on the $|0_L\rangle$ and $|1_L\rangle$ manifold of states, we may write B as

$$B = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} = e^{i\theta Y}\,. \tag{7.35}$$

Phase shifters and beamsplitters together allow arbitrary single qubit operations to be performed to our optical qubit. This a consequence of Theorem 4.1 on page 175, which states that all single qubit operations can be generated from $\hat{z}$-axis rotations $R_z(\alpha) = \exp(-i\alpha Z/2)$, and $\hat{y}$-axis rotations, $R_y(\alpha) = \exp(-i\alpha Y/2)$. A phase shifter performs R_z rotations, and a beamsplitter performs R_y rotations.

Exercise 7.9: (Optical Hadamard gate) Show that the following circuit acts as a Hadamard gate on dual-rail single photon states, that is, $|01\rangle \to (|01\rangle + |10\rangle)/\sqrt{2}$ and $|10\rangle \to (|01\rangle - |10\rangle)/\sqrt{2}$ up to an overall phase:



Exercise 7.10: (Mach–Zehnder interferometer) Interferometers are optical tools used to measure small phase shifts, which are constructed from two beamsplitters. Their basic principle of operation can be understood by this simple exercise.

1. Note that this circuit performs the identity operation:

Box 7.3: $SU(2)$ Symmetry and quantum beamsplitters

There is an interesting connection between the Lie group $SU(2)$ and the algebra of two coupled harmonic oscillators, which is useful for understanding the quantum beamsplitter transformation. Identify

$$a^\dagger a - b^\dagger b \to Z \tag{7.36}$$

$$a^\dagger b \to \sigma_+ \tag{7.37}$$

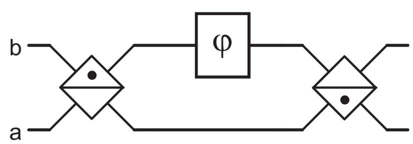
$$ab^\dagger \to \sigma_- \,, \tag{7.38}$$

where Z is the Pauli operator, and $\sigma_\pm = (X \pm iY)/2$ are raising and lowering operators defined in terms of Pauli X and Y. From the commutation relations for a, $a^\dagger$, b, and $b^\dagger$, it is easy to verify that these definitions satisfy the usual commutation relations for the Pauli operators, (2.40). Also note that the total number operator, $a^\dagger a + b^\dagger b$, commutes with σ_z, σ_+, and σ_-, as it should, being an invariant quantity under rotations in the $SU(2)$ space. Using $X = a^\dagger b + ab^\dagger$ and $Y = -i(a^\dagger b - ab^\dagger)$ in the traditional $SU(2)$ rotation operator

$$R(\hat{n}, \theta) = e^{-i\theta\vec{\sigma}\cdot\hat{n}/2} \tag{7.39}$$

gives us the desired beamsplitter operator when $\hat{n}$ is taken to be the $-\hat{y}$-axis.

2. Compute the rotation operation (on dual-rail states) which this circuit performs, as a function of the phase shift φ:



Exercise 7.11: What is $B|2,0\rangle$ for $\theta = \pi/4$?

Exercise 7.12: **(Quantum beamsplitter with classical inputs)** What is $B|\alpha\rangle|\beta\rangle$ where $|\alpha\rangle$ and $|\beta\rangle$ are two coherent states as in Equation (7.16)? (*Hint*: recall that $|n\rangle = \frac{(a^\dagger)^n}{\sqrt{n!}}|0\rangle$.)

Nonlinear Kerr media. The most important effect of a Kerr medium is the *cross phase modulation* it provides between two modes of light. That is classically described by the n_2 term in (7.19), which is effectively an interaction between photons, mediated by atoms in the Kerr medium. Quantum-mechanically, this effect is described by the Hamiltonian

$$H_{xpm} = -\chi a^\dagger a b^\dagger b \,, \tag{7.40}$$

where a and b describe two modes propagating through the medium, and for a crystal of length L we obtain the unitary transform

$$K = e^{i\chi L a^\dagger a b^\dagger b}. \tag{7.41}$$

χ is a coefficient related to n_2, and the third order nonlinear susceptibility coefficient usually denoted as $\chi^{(3)}$. That the expected classical behavior arises from this Hamiltonian is left as Exercise 7.14 for the reader.

By combining Kerr media with beamsplitters, a controlled-NOT gate can be constructed in the following manner. For single photon states, we find that

$$K|00\rangle = |00\rangle \tag{7.42}$$
$$K|01\rangle = |01\rangle \tag{7.43}$$
$$K|10\rangle = |10\rangle \tag{7.44}$$
$$K|11\rangle = e^{i\chi L}|11\rangle\,, \tag{7.45}$$

and let us take $\chi L = \pi$, such that $K|11\rangle = -|11\rangle$. Now consider two dual-rail states, that is, four modes of light. These live in a space spanned by the four basis states $|e_{00}\rangle = |1001\rangle$, $|e_{01}\rangle = |1010\rangle$, $|e_{10}\rangle = |0101\rangle$, $|e_{11}\rangle = |0110\rangle$. Note that we have flipped the usual order of the two modes for the first pair, for convenience (physically, the two modes are easily swapped using mirrors). Now, if a Kerr medium is applied to act upon the two middle modes, then we find that $K|e_i\rangle = |e_i\rangle$ for all i except $K|e_{11}\rangle = -|e_{11}\rangle$. This is useful because the controlled-NOT operation can be factored into

$$\underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}}_{U_{CN}} = \underbrace{\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}}_{I\otimes H} \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}}_{K} \underbrace{\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}}_{I\otimes H}, \tag{7.46}$$

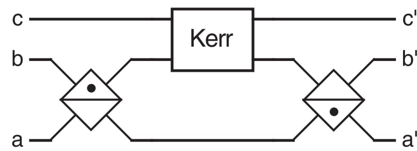
where H is the single qubit Hadamard transform (simply implemented with beamsplitters and phase shifters), and K is the Kerr interaction we just considered, with $\chi L = \pi$. Such an apparatus has been considered before, for constructing a reversible classical optical logic gate, as described in Box 7.4; in the single photon regime, it also functions as a quantum logic gate.

Summarizing, the CNOT can be constructed from Kerr media, and arbitrary single qubit operations realized using beamsplitters and phase shifters. Single photons can be created using attenuated lasers, and detected with photodetectors. Thus, in theory, a quantum computer can be implemented using these optical components!

Exercise 7.13: (Optical Deutsch–Jozsa quantum circuit) In Section 1.4.4 (page 34), we described a quantum circuit for solving the one-bit Deutsch–Jozsa problem. Here is a version of that circuit for single photon states (in the dual-rail representation), using beamsplitters, phase shifters, and nonlinear Kerr media:

Box 7.4: The quantum optical Fredkin gate

An optical Fredkin gate can be built using two beamsplitters and a nonlinear Kerr medium as shown in this schematic diagram:



This performs the unitary transform $U = B^\dagger K B$, where B is a 50/50 beamsplitter, K is the Kerr cross phase modulation operator $K = e^{i\xi\, b^\dagger b\, c^\dagger c}$, and $\xi = \chi L$ is the product of the coupling constant and the interaction distance. This simplifies to give

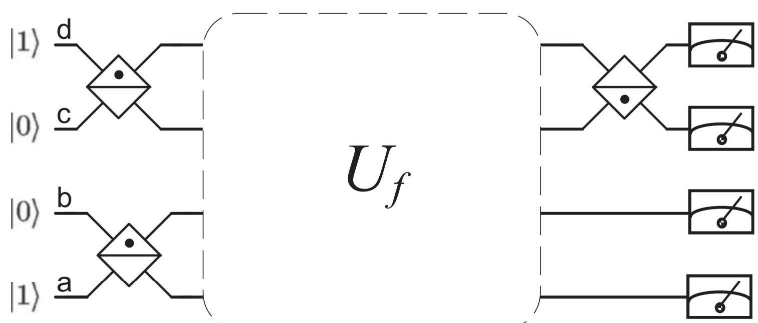
$$U = \exp\left[i\xi c^\dagger c \left(\frac{b^\dagger - a^\dagger}{2}\right)\left(\frac{b-a}{2}\right)\right] \tag{7.47}$$

$$= e^{i\frac{\pi}{2}b^\dagger b}\, e^{\frac{\xi}{2}c^\dagger c(a^\dagger b - b^\dagger a)}\, e^{-i\frac{\pi}{2}b^\dagger b}\, e^{i\frac{\xi}{2}a^\dagger a\, c^\dagger c}\, e^{i\frac{\xi}{2}b^\dagger b\, c^\dagger c}\,. \tag{7.48}$$

The first and third exponentials are constant phase shifts, and the last two phase shifts come from cross phase modulation. All those effects are not fundamental, and can be compensated for. The interesting term is the second exponential, which is defines the quantum Fredkin operator

$$F(\xi) = \exp\left[\frac{\xi}{2}c^\dagger c\,(a^\dagger b - b^\dagger a)\right]\,. \tag{7.49}$$

The usual (classical) Fredkin gate operation is obtained for $\xi = \pi$, in which case when no photons are input at c, then $a' = a$ and $b' = b$, but when a single photon is input at c, then $a' = b$ and $b' = a$. This can be understood by realizing that $F(\chi)$ is like a controlled-beamsplitter operator, where the rotation angle is $\xi c^\dagger c$. Note that this description does not use the dual-rail representation; in that representation, this Fredkin gate corresponds to a controlled-NOT gate.



1. Construct circuits for the four possible classical functions U_f using Fredkin gates and beamsplitters.
2. Why are no phase shifters necessary in this construction?
3. For each U_f show explicitly how interference can be used to explain how the quantum algorithm works.

4. Does this implementation work if the single photon states are replaced by coherent states?

Exercise 7.14: (Classical cross phase modulation) To see that the expected classical behavior of a Kerr medium is obtained from the definition of K, Equation (7.41), apply it to two modes, one with a coherent state and the other in state $|n\rangle$; that is, show that

$$K|\alpha\rangle|n\rangle = |\alpha e^{i\chi L n}\rangle|n\rangle \,. \tag{7.50}$$

Use this to compute

$$\rho_a = \mathrm{Tr}_b \left[K|\alpha\rangle|\beta\rangle\langle\beta|\langle\alpha|K^\dagger\right] \tag{7.51}$$

$$= e^{-|\beta|^2} \sum_m \frac{|\beta|^{2m}}{m!} |\alpha e^{i\chi L m}\rangle\langle\alpha e^{i\chi L m}| \,, \tag{7.52}$$

and show that the main contribution to the sum is for $m = |\beta|^2$.

7.4.3 Drawbacks

The single photon representation of a qubit is attractive. Single photons are relatively simple to generate and measure, and in the dual-rail representation, arbitrary single qubit operations are possible. Unfortunately, interacting photons is difficult – the best nonlinear Kerr media available are very weak, and cannot provide a cross phase modulation of π between single photon states. In fact, because a nonlinear index of refraction is usually obtained by using a medium near an optical resonance, there is always some absorption associated with the nonlinearity, and it can theoretically be estimated that in the best such arrangement, approximately 50 photons must be absorbed for each photon which experiences a π cross phase modulation. This means that the outlook for building quantum computers from traditional nonlinear optics components is slim at best.

Nevertheless, from studying this optical quantum computer, we have gained some valuable insight into the nature of the *architecture* and system design of a quantum computer. We now can see what an actual quantum computer might look like in the laboratory (if only sufficiently good components were available to construct it), and a striking feature is that it is constructed nearly completely from optical interferometers. In the apparatus, information is encoded both in the photon number and the phase of the photon, and interferometers are used to convert between the two representations. Although it is feasible to construct stable optical interferometers, if an alternate, massive representation of a qubit were chosen, then it could rapidly become difficult to build stable interferometers because of the shortness of typical de Broglie wavelengths. Even with the optical representation, the multiple interlocked interferometers which would be needed to realize a large quantum algorithm would be a challenge to stabilize in the laboratory.

Historically, optical *classical* computers were once thought to be promising replacements for electronic machines, but they ultimately failed to live up to expectations when sufficiently nonlinear optical materials were not discovered, and when their speed and parallelism advantages did not sufficiently outweigh their alignment and power disadvantages. On the other hand, optical communications is a vital and important area; one reason for this is that for distances longer than one centimeter, the energy needed to transmit a bit using a photon over a fiber is smaller than the energy required to charge a typical 50 ohm electronic transmission line covering the same distance. Similarly, it may be that optical qubits may find a natural home in communication of quantum information, such as in quantum cryptography, rather than in computation.

Despite the drawbacks facing optical quantum computer realizations, the theoretical formalism which describes them is absolutely fundamental in all the other realizations we shall study in the remainder of this chapter. In fact, you may think of what we shall turn to next as being just another kind of optical quantum computer, but with a different (and better!) kind of nonlinear medium.

Optical photon quantum computer

- **Qubit representation**: Location of single photon between two modes, $|01\rangle$ and $|10\rangle$, or polarization.
- **Unitary evolution**: Arbitrary transforms are constructed from phase shifters (R_z rotations), beamsplitters (R_y rotations), and nonlinear Kerr media, which allow two single photons to cross phase modulate, performing $\exp\left[i\chi L|11\rangle\langle 11|\right]$.
- **Initial state preparation**: Create single photon states (e.g. by attenuating laser light).
- **Readout**: Detect single photons (e.g. using a photomultipler tube).
- **Drawbacks**: Nonlinear Kerr media with large ratio of cross phase modulation strength to absorption loss are difficult to realize.

7.5 Optical cavity quantum electrodynamics

Cavity quantum electrodynamics (QED) is a field of study which accesses an important regime involving coupling of single atoms to only a few optical modes. Experimentally, this is made possible by placing single atoms within optical cavities of very high Q; because only one or two electromagnetic modes exist within the cavity, and each of these has a very high electric field strength, the dipole coupling between the atom and the field is very high. Because of the high Q, photons within the cavity have an opportunity to interact many times with the atoms before escaping. Theoretically, this technique presents a unique opportunity to control and study single quantum systems, opening many opportunities in quantum chaos, quantum feedback control, and quantum computation.

In particular, single-atom cavity QED methods offer a potential solution to the dilemma with the optical quantum computer described in the previous section. Single photons can be good carriers of quantum information, but they require some other medium in order to interact with each other. Because they are bulk materials, traditional nonlinear optical Kerr media are unsatisfactory in satisfying this need. However, well isolated single atoms might not necessarily suffer from the same decoherence effects, and moreover, they could also provide cross phase modulation between photons. In fact, what if the state of single photons could be efficiently transfered to and from single atoms, whose interactions could be controlled? This potential scenario is the topic of this section.