Answers to exercises

Here we provide answers to all the exercises in the book; in some cases we only provide brief numerical answers, while in other cases we provide more explanation.

Part I: Quantum information

1. Quantum bits and quantum gates

1. This follows by direct matrix calculation:

$$|\psi\rangle\langle\psi| = \begin{pmatrix} \cos(\theta/2) \\ \sin(\theta/2)\mathrm{e}^{\mathrm{i}\phi} \end{pmatrix} \begin{pmatrix} \cos(\theta/2) & \sin(\theta/2)\mathrm{e}^{-\mathrm{i}\phi} \end{pmatrix} \tag{A.1}$$

$$= \begin{pmatrix} \cos^2(\theta/2) & \sin(\theta/2)\cos(\theta/2)\mathrm{e}^{-\mathrm{i}\phi} \\ \sin(\theta/2)\cos(\theta/2)\mathrm{e}^{\mathrm{i}\phi} & \sin^2(\theta/2) \end{pmatrix} \tag{A.2}$$

$$= \frac{1}{2}\begin{pmatrix} \cos\theta + 1 & \sin\theta(\cos\phi - \mathrm{i}\sin\phi) \\ \sin\theta(\cos\phi + \mathrm{i}\sin\phi) & -\cos\theta + 1 \end{pmatrix} \tag{A.3}$$

$$= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{\cos\theta}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + \frac{\sin\theta\cos\phi}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \frac{\sin\theta\sin\phi}{2}\begin{pmatrix} 0 & -\mathrm{i} \\ i & 0 \end{pmatrix} \tag{A.4}$$

$$= \tfrac{1}{2}\left(\sigma_0 + s_x\,\sigma_x + s_y\,\sigma_y + s_z\,\sigma_z\right) \tag{A.5}$$

with $s_x = \sin\theta\cos\phi$, $s_y = \sin\theta\sin\phi$, and $s_z = \cos\theta$. Thus

$$\mathbf{s}.\mathbf{s} = \sin^2\theta\cos^2\phi + \sin^2\theta\sin^2\phi + \cos^2\theta = 1. \tag{A.6}$$

As $\mathbf{s}$ is a unit vector, it connects the origin with a point on the unit sphere.

2. A mixed state has the form $\rho = \sum_n P_n|\psi_n\rangle\langle\psi_n|$, where $P_n \geq 0$ and $\sum_n P_n = 1$. Each contributing density matrix can be described by a Bloch vector and so the mixed state can also be represented by a vector $\mathbf{s} = \sum_n P_n\mathbf{s}_n$. As all the $\mathbf{s}_n$ are of unit length, the weighted sum has a length of at most 1 (which only occurs when all the P_n except one are zero). Thus the mixed-state vector lies *inside* the unit sphere (the Bloch sphere). The point $\frac{1}{2}\sigma_0$ corresponds to the center of the Bloch sphere. This is the *maximally mixed state*.
3. The conventional description of the maximally mixed state has the matrix form

$$\rho_{MM} = \tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1| = \tfrac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \tfrac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \tfrac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \tfrac{1}{2}\mathbb{1}. \tag{A.7}$$

Similarly an equal mixture of $|+\rangle$ and $|-\rangle$ takes the form

$$\tfrac{1}{2}|+\rangle\langle+| + \tfrac{1}{2}|-\rangle\langle-| = \tfrac{1}{2}\begin{pmatrix}\frac{1}{2} & \frac{1}{2}\\ \frac{1}{2} & \frac{1}{2}\end{pmatrix} + \tfrac{1}{2}\begin{pmatrix}\frac{1}{2} & -\frac{1}{2}\\ -\frac{1}{2} & \frac{1}{2}\end{pmatrix} = \tfrac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \rho_{MM}. \quad \text{(A.8)}$$

4. The result calculated above is obvious if the states are represented by Bloch vectors. The vectors representing the orthogonal states $|0\rangle$ and $|1\rangle$ are *antiparallel* on the Bloch sphere, and so an equally weighted sum gives the null vector, corresponding to a point at the center of the Bloch sphere, that is the maximally mixed state. Similarly the vectors representing $|+\rangle$ and $|-\rangle$ are also antiparallel, and so sum to give the same result. Clearly, the maximally mixed state can be decomposed as an equal mixture of any state $|\psi\rangle$ with the state $|\psi^{\perp}\rangle$ which is orthogonal to it, and so there are an infinite number of decompositions into two equally weighted parts. (Of course, further, even more complex decompositions are also possible.)
5. By direct multiplication $\sigma_x^2 = \sigma_0$ and similarly for σ_y and σ_z. Now

$$\exp(-\mathrm{i}\theta\,\sigma_\alpha/2) = \sigma_0 + \left(\frac{-\mathrm{i}\theta/2}{1}\right)\sigma_\alpha + \left(\frac{(-\mathrm{i}\theta/2)^2}{2}\right)\sigma^2\alpha + \left(\frac{(-\mathrm{i}\theta/2)^3}{3!}\right)\sigma^3\alpha + \ldots \quad \text{(A.9)}$$

$$= \sigma_0 - \mathrm{i}\left(\frac{\theta/2}{1}\right)\sigma_\alpha - \left(\frac{(\theta/2)^2}{2}\right)\sigma_0 - \mathrm{i}\left(\frac{(-\theta/2)^3}{3!}\right)\sigma\alpha + \ldots \quad \text{(A.10)}$$

$$= \sigma_0\left(1 - \frac{(\theta/2)^2}{2} + \ldots\right) - \mathrm{i}\sigma_\alpha\left(\theta/2 - \frac{(\theta/2)^3}{3!} + \ldots\right) \quad \text{(A.11)}$$

$$= \sigma_0\cos(\theta/2) - \mathrm{i}\sigma_\alpha\sin(\theta/2). \quad \text{(A.12)}$$

6. Using methods from above we note that the propagator for 90_y is $(\sigma_0 - \mathrm{i}\sigma_y)/\sqrt{2}$, while that for 180_x is $-\mathrm{i}\sigma_x$. Then use brute-force multiplication (note the order!):

$$\frac{-\mathrm{i}}{\sqrt{2}}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix} = \frac{-\mathrm{i}}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \quad \text{(A.13)}$$

which is the Hadamard gate (up to an irrelevant global phase). The other three are done in the same way.
7. $\mathrm{H}\sigma_x\mathrm{H} = \mathrm{H}\,(\mathrm{H}\sigma_z\mathrm{H})\,\mathrm{H} = (\mathrm{HH})\,\sigma_z\,(\mathrm{HH}) = \mathbb{1}\sigma_z\mathbb{1} = \sigma_z$.
8. Reversing the definitions of $|+\rangle$ and $|-\rangle$ gives $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$ and $|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$, so

$$|\psi\rangle = \left(\frac{\alpha+\beta}{\sqrt{2}}\right)|+\rangle + \left(\frac{\alpha-\beta}{\sqrt{2}}\right)|-\rangle \quad \text{(A.14)}$$

and making an X-measurement returns $|+\rangle$ or $|-\rangle$ with probabilities

$$P_+ = \left|\frac{\alpha+\beta}{\sqrt{2}}\right|^2 \qquad P_- = \left|\frac{\alpha-\beta}{\sqrt{2}}\right|^2. \quad \text{(A.15)}$$

Alternatively we have

$$\mathrm{H}|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}\alpha+\beta\\ \alpha-\beta\end{pmatrix} \quad \text{(A.16)}$$

and making a Z-measurement gives $|0\rangle$ or $|1\rangle$ with probabilities as above; applying a final Hadamard gate simply converts these to $|+\rangle$ and $|-\rangle$ with the same probabilities.

9. The first Hadamard gate rotates the two eigenstates of the X-measurement onto the two eigenstates of a Z-measurement. Any single-qubit measurement will have two eigenstates which lie at diametrically opposed points on the Bloch sphere and which can be rotated onto $|0\rangle$ and $|1\rangle$ in the same way. As rotation gates are unitary they will also work with superposition states. Equivalently, we can think of unitary gates as rotating operators rather than states: surrounding a Z-measurement gate with a pair of Hadamard gates is equivalent to rotating it into an X-measurement.

2. An atom in a laser field

1. In systems of this kind the single outer electron can be thought of as moving in a central field, although the form of this field will be much more complex than the simple Coulomb field found in hydrogen, and so the wavefunction will still be separable into radial and angular parts. As the selection rules only rely on certain angular integrals being zero, they will be unaffected by the changes to the radial parts.
2. Inserting the numbers gives $1/\Gamma \approx 31$ ns. To achieve Rabi flopping we need $V \gg \Gamma$, and using $E = \hbar V/a_0 e$ gives $E \gg 400$ V for the *rotating* field; double this for the oscillating field. In reality the lifetime is about 7 ns, and the field must be large compared with 5000 V/m.
3. Sudden jumps are only effective when $V \gtrsim \omega_0$ or $E \gtrsim 2\pi\hbar c/ea_0\lambda$, and putting the numbers in gives $E \gtrsim 6 \times 10^{10}$ V/m, which is too large to generate as a static field (breakdown will occur). Even if you could produce the field it would cause many other transitions as well.
4. The Abbe limit is $\lambda/2 \approx 200$ nm (realistic systems are often around an order of magnitude worse than this).
5. For the excited state population, compare the energy gap $E = hc/\lambda \approx 5 \times 10^{-19}$ J with $k_B T \approx 4.1 \times 10^{-21}$ J at 300 K; clearly the excited state population will be negligible.
6. To get a peak electric field strength of 800 V/m in a spot of diameter 200 nm requires a power of 13 pW; the surprisingly low power requirement largely reflects the tiny size of the laser spot. This calculation is fairly unrealistic, both as to the field strength required and the spot size achievable: using more realistic numbers of 10,000 V/m and a diameter of 10 μm gives a power of 5 μW, which is still rather low. Significantly larger powers are used in real quantum computers as this enables Raman transitions to be used far from resonance.

3. Spins in magnetic fields

1. This can be worked out by brute force but it is simpler just to rescale the field. If a 90° rotation lasts 6 μs then a 360° rotation lasts 24 μs, and the rotation rate is $10^6/24$ Hz. Divide this by 500 MHz and multiply by 12 T to get 1 mT or 10 Gauss. But this is the strength of the *rotating* field, and we want the oscillating field, so double this to get 2 mT or 20 Gauss.

2. Using $E = h\nu$ with $\nu = 500\,\text{MHz}$ gives an energy gap of $3.313 \times 10^{-25}\,\text{J}$ or $2\,\mu\text{eV}$. Compare this with $k_B T$ at 300 K, which is $4.142 \times 10^{-21}\,\text{J}$, so the two states will be very nearly equally occupied. A Boltzmann calculation gives fractional populations of 0.50002 and 0.49998, with an excess fractional population of 4×10^{-5}.
3. In a sample of 0.2 ml of water there are about $0.2/18$ moles of water, which is 6.7×10^{21} molecules, but each molecule has two hydrogen atoms, giving 1.34×10^{22} nuclei. Thus the excess population is 5.35×10^{17} spins. For the last bit, solve the Boltzmann equation to discover that 99% population in the lower state requires $h\nu/k_B T = 4.595$, or a temperature of 5 mK.
4. The answer depends on what is meant by "tolerate," but suppose we insist that the inhomogeneous broadening can be no more than 50% as large as the homogeneous broadening, that is 0.5 Hz. To achieve this at a frequency of 0.5 GHz requires a field homogeneous to one part in 10^9. Reaching this limit is difficult and expensive, but possible over small regions of space.
5. Begin by finding the propagators for the underlying gates:

$$\phi_z = \begin{pmatrix} e^{-i\phi/2} & 0 \\ 0 & e^{i\phi/2} \end{pmatrix} \qquad 180_x = -i\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad 180_y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{A.17}$$

and the first result is shown by direct multiplication:

$$\phi_z\, 180_x\, \phi_z = -i\begin{pmatrix} e^{-i\phi/2} & 0 \\ 0 & e^{i\phi/2} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} e^{-i\phi/2} & 0 \\ 0 & e^{i\phi/2} \end{pmatrix} \tag{A.18}$$

$$= -i\begin{pmatrix} e^{-i\phi/2} & 0 \\ 0 & e^{i\phi/2} \end{pmatrix}\begin{pmatrix} 0 & e^{i\phi/2} \\ e^{-i\phi/2} & 0 \end{pmatrix} = -i\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{A.19}$$

which is identical to 180_x. The propagator for the second spin-echo sequence is just the square of the above, and $(-i\sigma_x)^2 = -\mathbb{1}$, which is the identity up to a global phase. The third and fourth sequences give the same result. Direct multiplication shows that changing the phase of both 180 pulses has no effect, but changing just one of them gives $-i\sigma_z$, which is a 180_z rotation. In general, using 180 pulses separated by a phase angle is equivalent to performing a z-rotation through twice that angle.

4. Photon techniques

1. We have the general form for $U(\theta, \phi)$ in equation (4.13) and a half wave plate corresponds to $\phi = \pi$, so

$$U(\theta, \pi) = \begin{pmatrix} \cos^2\theta - \sin^2\theta & 2\cos\theta\sin\theta \\ 2\cos\theta\sin\theta & -\cos^2\theta + \sin^2\theta \end{pmatrix} = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix}. \tag{A.20}$$

Now choosing $2\theta = \pi/2$ gives $U(\pi/4, \pi) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ which is a NOT gate, while choosing $2\theta = \pi/4$ gives

$$U(\pi/8, \pi) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{A.21}$$

which is a Hadamard gate.

2. As the number states are all orthonormal we have

$$\langle\alpha|\alpha\rangle = \mathrm{e}^{-|\alpha|^2}\sum_{n=0}^{\infty}\frac{(\alpha^*\alpha)^n}{n!} = \mathrm{e}^{-|\alpha|^2}\mathrm{e}^{+|\alpha|^2} = 1 \tag{A.22}$$

and $P(n) = \mathrm{e}^{-|\alpha|^2}|\alpha|^{2n}/n!$. Hence $P(0) = \mathrm{e}^{-|\alpha|^2}$, $P(1) = |\alpha|^2 P(0)$, and $P(n > 0) = 1 - P(0)$. Thus if a laser pulse contains at least one photon then the probability that it contains exactly one photon is

$$P(n = 1|n > 0) = \frac{|\alpha|^2\mathrm{e}^{-|\alpha|^2}}{1 - \mathrm{e}^{-|\alpha|^2}} \tag{A.23}$$

and for $\alpha = \sqrt{0.1}$ we get $P(0) = 0.9048$, $P(1) = 0.0905$, and $P(n = 1|n > 0) = 0.9508$.

5. Two qubits and beyond

1. Start by writing the controlled-NOT gate as $|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \mathrm{X}$. Then note that $\mathrm{X} = \mathrm{HZH}$, and that $\mathbb{1}$ can be written as $\mathrm{H}\mathbb{1}\mathrm{H}$. Finally, factor out the common Hadamard gate to leave $(\mathbb{1} \otimes \mathrm{H}) \cdot (|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \mathrm{Z}) \cdot (\mathbb{1} \otimes \mathrm{H})$ as desired.
2. Start from a general eigenstate $|a\rangle|b\rangle$ and follow through the sequence to three controlled-NOT gates in turn using $a \oplus a \oplus b = 0 \oplus b = b$ to simplify terms:

$$|a\rangle|b\rangle \to |a\rangle|a\oplus b\rangle \to |a\oplus(a\oplus b)\rangle|a\oplus b\rangle = |b\rangle|a\oplus b\rangle \to |b\rangle|(a\oplus b)\oplus b\rangle = |b\rangle|a\rangle. \tag{A.24}$$

   The final part follows immediately from the linearity of unitary operations. This is normally thought of as swapping amplitudes between the two qubits, but it is often better to think of this process as swapping the labels identifying the two qubits.
3. The matrix form of the SWAP gate

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{A.25}$$

   can be obtained either by matrix multiplication or by noting directly that it swaps $|01\rangle$ and $|10\rangle$ and leaves $|00\rangle$ and $|11\rangle$ alone. Explicit calculation shows that the SWAP gate leaves three Bell states entirely unaffected, except that the singlet state $|\psi^-\rangle$ picks up a global phase factor of -1. The result is not surprising as the Bell states are symmetric or antisymmetric states of the two qubits as a whole, not of the individual qubits, and so should not be affected by swapping the labels of the qubits. The global phase of -1 for $|\psi^-\rangle$ occurs because this state is antisymmetric under the exchange of qubit labels.
4. The explicit forms are

$$|00\rangle = \frac{|\phi^+\rangle + |\phi^-\rangle}{\sqrt{2}} \qquad |11\rangle = \frac{|\phi^+\rangle - |\phi^-\rangle}{\sqrt{2}}, \tag{A.26}$$

$$|01\rangle = \frac{|\psi^+\rangle + |\psi^-\rangle}{\sqrt{2}} \qquad |10\rangle = \frac{|\psi^+\rangle - |\psi^-\rangle}{\sqrt{2}}. \tag{A.27}$$

   Just as superpositions of separable states can be entangled, so superpositions of entangled states can be separable.

5. Direct calculation shows that starting from $|1\rangle|0\rangle$ gives $|\phi^-\rangle$. Similarly, starting from $|0\rangle|1\rangle$ and $|1\rangle|1\rangle$ gives $|\psi^+\rangle$ and $|\psi^-\rangle$, respectively.
6. Simply apply the gates in the entangling network in reverse order to disentangle the states. This works because both controlled-NOT and H are self-inverse; in general, you would have to use inverse gates as well as reversing the order.

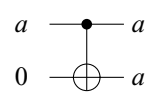
6. Measurement and entanglement

1. This problem is almost identical to the series of polarizers considered previously; the angles on the Bloch sphere are twice those between the axes of light polarization, but this cancels out. Hence the probability that the quantum state is always projected onto $|0\rangle$ is $P_n = [\cos(\pi/2n)]^{2n}$, and a series expansion gives $P_n \approx 1 - \pi^2/4n$. In the limit of very large n the quantum state will always be found in $|0\rangle$. Note that this is only a lower bound on the probability that the final state will be $|0\rangle$, as the state could go from $|0\rangle$ to $|1\rangle$ and then back to $|0\rangle$, but in the limit of large n such double changes will be very unlikely.
2. Ignoring global phases a Z gate will turn $|\psi^-\rangle$ into $|\psi^+\rangle$, while an X gate will turn it into $|\phi^-\rangle$. To obtain $|\phi^+\rangle$ either apply both X and Z gates in either order, or note that this combination is equivalent to Y.
3. Clearly it suffices to show that $|\psi^-\rangle$ is unaffected by bilateral Hadamards and T gates (H $\otimes$ H and T $\otimes$ T). These are easily shown by direct calculation.
4. Measurement in any basis can be achieved by applying some rotation to the qubit before and after the measurement, and if the measurement bases are the same for each qubit then the rotations must be the same for each qubit. But this is a bilateral rotation, and we have just shown that $|\psi^-\rangle$ is invariant under bilateral rotations. The final state after the measurement will be affected by the second bilateral rotation, but this does not affect the outcome of the measurements. This argument does not work for the other four Bell states as they are not invariant under bilateral rotations: for example, $|\phi^\pm\rangle$ are interconverted by bilateral T gates, while $|\phi^-\rangle$ and $|\psi^+\rangle$ are interconverted by bilateral Hadamard gates.

Part II: Quantum computation

7. Principles of quantum computing

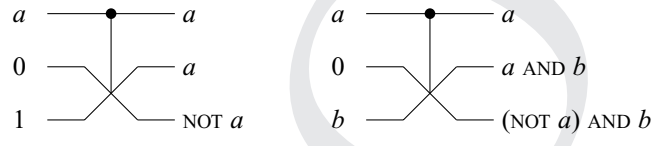
1. The SWAP gate was explored in Part I and can be implemented using the network shown in equation (5.12), which works for both classical and quantum inputs. The classical CLONE network is just a single controlled-NOT gate



(A.28)

(if $a = 1$ then the second qubit is flipped from 0 to 1) but CLONE does not work on a quantum computer unless the qubits are in eigenstates: the no-cloning theorem.

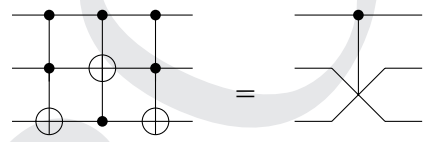
2. To build NOT and controlled-NOT gates from Toffoli gates just set both inputs (NOT) or one of the two inputs (controlled-NOT) to one. To build an OR gate use De Morgan's laws, a OR $b =$ NOT(NOT a AND NOT b) and implement AND using a Toffoli gate.
3. Both NOT and AND gates can be built from Fredkin gates with appropriate patterns of inputs, though it takes a bit of thought to see why these gates work.



(A.29)

The circuit for a NOT gate also copies the input a at the same time, and so implements CLONE on a classical computer.

4. Since the Fredkin gate is a controlled-SWAP gate it can be built from the standard SWAP network by adding an additional control to each gate, turning each controlled-NOT gate into a Toffoli gate:



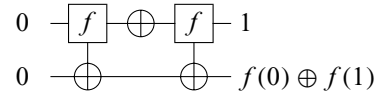
(A.30)

It is not possible to build a Toffoli gate using only Fredkin gates without using ancilla bits; this is most easily seen by noting that the Fredkin gate only swaps bits or leaves them alone, so the number of 0s and 1s in the output must be the same as in the input. However, since the Fredkin gate is *universal*, there must be some construction of a Toffoli gate using multiple Fredkin gates and ancilla bits.

5. If the control bit is 0 then the central controlled-gate is not applied to the target qubit, which just experiences $VV^\dagger = \mathbb{1}$; if the control bit is 1 the target qubit experiences $VUV^\dagger$ as desired. This idea obviously generalizes to controlled-controlled-gates, and since controlled-NOT is self-inverse we can simplify the construction in equation (A.30) by replacing the outer Toffoli gates by simple controlled-NOT gates.
6. As previously noted the controlled-NOT gate implements the bitwise sum, that is the sum without carry, while the carry bit is 1 if and only if both a and b are 1. There is no need to explicitly preserve the second input as all gates applied to it are reversible.

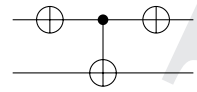
8. Elementary quantum algorithms

1. The oracle will take the form of an f-controlled-NOT gate, and its parity can be determined in two calls with just two bits:



(A.31)

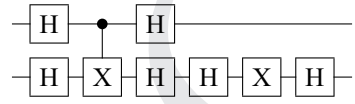
2. The circuit



(A.32)

will achieve the desired result.

3. We have already proved f_{11} and f_{01}, and f_{00} is trivial, so the only interesting case is f_{10}. Using $\mathrm{H}^2 = \mathbb{1}$ the circuit can be written as



(A.33)

and the remaining steps follow easily by combining results for f_{01} and f_{11}.

4. The amplitude amplification operator is given by

$$U_{AA} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \tag{A.34}$$

$$= \frac{1}{2}\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix}. \tag{A.35}$$

Suppose the satisfying function is f_{00}; the state after the function evaluation will be

$$\psi_{00} = \frac{1}{2}\begin{pmatrix} -1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \tag{A.36}$$

and the final state can then be evaluated by multiplication to get

$$U_{AA}\psi_{00} = \frac{1}{4}\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} -1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \tag{A.37}$$

which is $-|00\rangle$. The other three possibilities can be evaluated in exactly the same way, and the answers are obvious by symmetry.

5. For the case of two satisfying inputs, it is simplest to choose a concrete case again, such as f_{00} and f_{01} matching. Then explicit matrix calculations show that no amplitude amplification occurs: a measurement is equally likely to give any of the four possible results. As before, this argument applies whatever the two matches are. With three matches the situation is slightly more interesting, and amplitude amplification results in the final state being the single non-matching input, which now is the state marked with a unique phase.

6. Easily shown by direct calculation. As controlled-NOT gates are self-inverse the decoding networks can be obtained by applying the same gates in reverse order.
7. The state of the five qubits as they enter the network is

$$(\alpha|000\rangle + \beta|111\rangle) \otimes |0\rangle \otimes |0\rangle = \alpha|00000\rangle + \beta|11100\rangle \tag{A.38}$$

and in general we have four possible states:

$$\begin{aligned} |\psi_0\rangle \otimes |00\rangle &= \alpha|00000\rangle + \beta|11100\rangle, \\ |\psi_1\rangle \otimes |00\rangle &= \alpha|10000\rangle + \beta|01100\rangle, \\ |\psi_2\rangle \otimes |00\rangle &= \alpha|01000\rangle + \beta|10100\rangle, \\ |\psi_3\rangle \otimes |00\rangle &= \alpha|00100\rangle + \beta|11000\rangle, \end{aligned} \tag{A.39}$$

where the subscript identifies the bit which has experienced a spin flip error (0 indicating no error). Now run through the network of controlled-NOT gates:

$$\begin{aligned} |\psi_0\rangle \otimes |00\rangle &\xrightarrow{\mathrm{CN}_{14}} \alpha|00000\rangle + \beta|11110\rangle \xrightarrow{\mathrm{CN}_{24}} \alpha|00000\rangle + \beta|11100\rangle \\ &\xrightarrow{\mathrm{CN}_{15}} \alpha|00000\rangle + \beta|11101\rangle \xrightarrow{\mathrm{CN}_{35}} \alpha|00000\rangle + \beta|11100\rangle = |\psi_0\rangle \otimes |00\rangle, \end{aligned} \tag{A.40}$$

$$\begin{aligned} |\psi_1\rangle \otimes |00\rangle &\xrightarrow{\mathrm{CN}_{14}} \alpha|10010\rangle + \beta|01100\rangle \xrightarrow{\mathrm{CN}_{24}} \alpha|10010\rangle + \beta|01110\rangle \\ &\xrightarrow{\mathrm{CN}_{15}} \alpha|10011\rangle + \beta|01110\rangle \xrightarrow{\mathrm{CN}_{35}} \alpha|10011\rangle + \beta|01111\rangle = |\psi_1\rangle \otimes |11\rangle, \end{aligned} \tag{A.41}$$

$$\begin{aligned} |\psi_2\rangle \otimes |00\rangle &\xrightarrow{\mathrm{CN}_{14}} \alpha|01000\rangle + \beta|10110\rangle \xrightarrow{\mathrm{CN}_{24}} \alpha|01010\rangle + \beta|10110\rangle \\ &\xrightarrow{\mathrm{CN}_{15}} \alpha|01010\rangle + \beta|10111\rangle \xrightarrow{\mathrm{CN}_{35}} \alpha|01010\rangle + \beta|10110\rangle = |\psi_2\rangle \otimes |10\rangle, \end{aligned} \tag{A.42}$$

$$\begin{aligned} |\psi_3\rangle \otimes |00\rangle &\xrightarrow{\mathrm{CN}_{14}} \alpha|00100\rangle + \beta|11010\rangle \xrightarrow{\mathrm{CN}_{24}} \alpha|00100\rangle + \beta|11000\rangle \\ &\xrightarrow{\mathrm{CN}_{15}} \alpha|00100\rangle + \beta|11001\rangle \xrightarrow{\mathrm{CN}_{35}} \alpha|00101\rangle + \beta|11001\rangle = |\psi_3\rangle \otimes |01\rangle. \end{aligned} \tag{A.43}$$

The first three qubits (which are always control bits) are not changed by any of the controlled-NOT gates. Furthermore, the states of the ancilla qubits 4 and 5 are the same in both components of the superposition, and so can be factored out as indicated. If a quantum state is separable then measuring one part has no effect on the other, and so the ancillas can be measured without affecting the logical qubit. Finally, note that the four different ancilla states are all orthonormal, and so can be perfectly distinguished.

8. From the results of the previous question it is easy to write down the error correcting steps, as measuring the ancillas in the computational basis gives four distinct results with corresponding actions. For example, if the ancillas are in $|01\rangle$ then the encoded qubits are in state $|\psi_3\rangle$, which can be fixed by applying a NOT gate to qubit 3; similar results apply in the other cases. For quantum control, note that these actions can all be

implemented using generalized Toffoli gates, but implementing all these Toffoli gates is a lot of work. Another problem is that the ancilla qubits need to be reinitialized to $|0\rangle$ at the end; this is easy if the ancillas have been measured, as any ancillas in state $|1\rangle$ can be reset with NOT gates.

9. In a classical code, if two errors occur on different bits then two bits have the wrong value, and the majority vote approach "corrects" the third bit to the wrong value. (If the same bit is flipped both times then the situation is indistinguishable from the error-free case.) For the quantum code the state $|\psi_L\rangle$ is "corrected" to $\text{NOT}_L|\psi_L\rangle$.
10. For an initial state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ the relevant density matrices are

$$\rho_a = \tfrac{1}{2}\left(\phi_{+z}|\psi\rangle\langle\psi|\phi_{+z} + \phi_{-z}|\psi\rangle\langle\psi|\phi_{-z}\right) \tag{A.44}$$

and

$$\rho_b = (1-p)\times|\psi\rangle\langle\psi| + p\times \mathrm{Z}|\psi\rangle\langle\psi|\mathrm{Z}. \tag{A.45}$$

Now $\phi_{\pm z} = \cos(\phi/2)\mathbb{1} \mp \mathrm{i}\sin(\phi/2)\mathrm{Z}$ and so

$$\rho_a = \cos^2(\phi/2)|\psi\rangle\langle\psi| + \sin^2(\phi/2)\mathrm{Z}|\psi\rangle\langle\psi|\mathrm{Z} \tag{A.46}$$

with the other two terms canceling. Clearly ρ_a and ρ_b have the same form, and they are identical if $p = \sin^2(\phi/2)$, which rearranges to various forms such as $p = (1-\cos\phi)/2$ or $\phi = \arccos(1-2p)$.

9. More advanced quantum algorithms

1. There are four possible inputs, each of which has two possible outputs, giving a total of $2^4 = 16$ possible functions of which two are constant and six are balanced, with the last eight functions being neither constant nor balanced (four give mostly 0 and four give mostly 1). For the rest of the question we only consider the constant and balanced cases. A single value of $f(x)$ tells us nothing, while two values that disagree with each other indicates a balanced function. After three queries we know the result with certainty (either we have a disagreement, or three values are the same, and the function is constant). Hence the minimum number of queries is two and the maximum is three.

   For the average case, suppose the function is balanced and that $f(x_1) = 1$: then $f(x_2)$ will be 1 with probability $1/3$ and 0 with probability $2/3$. In the latter case we can stop; otherwise, we will need one more query. So for a balanced function the average number of queries required is $2/3\times 2 + 1/3\times 3 = 7/3$, while for a constant function it is always necessary to use three queries. If the function is chosen to be constant or balanced with 50% probability, then the average number of queries is $(7/3+3)/2 = 8/3$. (If the function was chosen from amongst the eight possible functions at random then the average query count would be $(6\times 7/3 + 2\times 3)/8 = 5/2$, but this is not what was asked!) On a quantum computer the minimum, maximum, and average query counts are all 1.
2. The angle θ can be calculated from equation (9.31) giving $\arctan(15/7) \approx 28.96^\circ$, while θ_0 is $\arcsin(1/\sqrt{15}) \approx 14.96^\circ$. The success probability is given by

$$P_r = \sin^2(\theta_0 + r\times\theta) \tag{A.47}$$

giving $P_0 \approx 0.067$, $P_1 \approx 0.481$, $P_2 \approx 0.708$, and $P_3 \approx 0.958$.

3. The values from the high N approximation are $\theta \approx 28.65^\circ$ (which is close to the exact value) and $\theta_0 = 0$ (which is not). The naive formula for choosing r gives slightly too high a value, but works well even for small N as the maximum in P_r is reasonably broad and (fortuitously) the effects of rounding r to the nearest integer go in the right direction when N is a low power of 2.
4. The first result is easily proven by direct calculation; the second result follows by linearity.
5. For $\mathcal{A} = \hbar\sigma_z$ and $\mathcal{B} = \hbar\sigma_x$ it is easy to calculate

$$\mathrm{e}^{-\mathrm{i}\mathcal{A}\delta t/\hbar} = \begin{pmatrix} \mathrm{e}^{-\mathrm{i}\delta t} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\delta t} \end{pmatrix} \qquad \mathrm{e}^{-\mathrm{i}\mathcal{B}\delta t/\hbar} = \begin{pmatrix} \cos\delta t & -\mathrm{i}\sin\delta t \\ -\mathrm{i}\sin\delta t & \cos\delta t \end{pmatrix} \tag{A.48}$$

and the approximate propagators follow by direct multiplication. The exact propagator can be calculated as

$$\mathrm{e}^{-\mathrm{i}(\mathcal{A}+\mathcal{B})\delta t/\hbar} = \frac{1}{\sqrt{2}} \begin{pmatrix} \sqrt{2}\cos(\sqrt{2}\delta t) - \mathrm{i}\sin(\sqrt{2}\delta t) & -\mathrm{i}\sin(\sqrt{2}\delta t) \\ -\mathrm{i}\sin(\sqrt{2}\delta t) & \sqrt{2}\cos(\sqrt{2}\delta t) + \mathrm{i}\sin(\sqrt{2}\delta t) \end{pmatrix} \tag{A.49}$$

either by brute force, or more subtly by noting that $\sigma_z + \sigma_x = \sqrt{2}\mathrm{H}$ and spotting the eigenvectors of H geometrically. The desired results then follow by taking series expansions.

10. Trapped atoms and ions

1. The potential energy is given by

$$U = \frac{M}{2}\sum_{n=1}^{N}\left(\omega_r^2 r_n^2 + \omega_z^2 z_n^2\right) + \frac{e^2}{4\pi\epsilon_0}\sum_{m>n}\frac{1}{|\mathbf{r}_n - \mathbf{r}_m|} \tag{A.50}$$

where the first group of terms is just the standard form for the potential energy of n harmonic oscillators, written in plane polar coordinates, and the second group of terms is the Coulomb repulsions between the ions (the second sum goes over all pairs of ions, counting each pair only once).
2. For an ion traveling in free space the effect of the motion will be to cause Doppler shifts in the transition frequencies. The effect will depend on the velocity distribution, but the most common result is Doppler broadening. In a trap the motion is quantized as vibrations within the trap, and it is necessary to consider transitions between vibrational sublevels of each electronic level. For a strictly harmonic trap these levels are equally spaced, with $E_n = (n + \frac{1}{2})h\nu$, and transitions with $\Delta n = \pm 1$ result in a pair of sharp sidebands, separated from the sharp principal transition by $\pm h\nu$.
3. The phase gate U_π negates $|01\rangle$ while leaving other states unchanged, and can be converted to the standard controlled-Z gate by applying X gates (NOT gates) to the first qubit before and after the U_π. Finally apply Hadamard gates to the second (target) qubit to get a controlled-NOT gate.

4. The first bit is just brute force:

$$|0\rangle\langle 0| \otimes \mathrm{Z} + |1\rangle\langle 1| \otimes \mathbb{1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = U_\pi. \tag{A.51}$$

Now the "massively entangled" state of two particles is just

$$U_\pi \mathrm{H}^{\otimes 2}|00\rangle = (|0\rangle\langle 0| \otimes \mathrm{Z} + |1\rangle\langle 1| \otimes \mathbb{1}) \times (|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle) \tag{A.52}$$

neglecting normalization. Multiplying this out gives

$$\begin{aligned} &|0\rangle\langle 0|0\rangle \otimes \mathrm{Z}|0\rangle + |0\rangle\langle 0|0\rangle \otimes \mathrm{Z}|1\rangle + |0\rangle\langle 0|1\rangle \otimes \mathrm{Z}|0\rangle + |0\rangle\langle 0|1\rangle \otimes \mathrm{Z}|1\rangle \\ &+|1\rangle\langle 1|0\rangle \otimes \mathbb{1}|0\rangle + |1\rangle\langle 1|0\rangle \otimes \mathbb{1}|1\rangle + |1\rangle\langle 1|1\rangle \otimes \mathbb{1}|0\rangle + |1\rangle\langle 1|1\rangle \otimes \mathbb{1}|1\rangle. \end{aligned} \tag{A.53}$$

As usual all the inner products can be replaced by 0 or 1, and dropping the (pointless) $\mathbb{1}$ operators this simplifies to

$$|0\rangle\mathrm{Z}|0\rangle + |0\rangle\mathrm{Z}|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle = (|0\rangle\mathrm{Z} + |1\rangle)(|0\rangle + |1\rangle). \tag{A.54}$$

The corresponding state for three atoms is

$$(|0\rangle\mathrm{Z} + |1\rangle)(|0\rangle\mathrm{Z} + |1\rangle)(|0\rangle + |1\rangle) \tag{A.55}$$

and multiplying this out and using $\mathrm{Z}|0\rangle = |0\rangle$ and $\mathrm{Z}|1\rangle = -|1\rangle$ gives

$$|0\rangle|0\rangle|0\rangle - |0\rangle|0\rangle|1\rangle - |0\rangle|1\rangle|0\rangle - |0\rangle|1\rangle|1\rangle + |1\rangle|0\rangle|0\rangle - |1\rangle|0\rangle|1\rangle + |1\rangle|1\rangle|0\rangle + |1\rangle|1\rangle|1\rangle, \tag{A.56}$$

matching the result given (neglecting normalization of course).

11. Nuclear magnetic resonance

1. From the exercises in Part I we know that a 12 T field gives a ^{1}H Larmor frequency of about 500 MHz, and so we need a field difference of $100 \div (500 \times 10^6) \times 12 = 2.4 \times 10^{-6}$ T per Å, or 24,000 T/m. Generating field gradients of this size is challenging.
2. There are two reasonable approaches to this. The first is to use perturbation theory, writing the Hamiltonian as $\mathcal{H} = \mathcal{H}_0 + \mathcal{H}_1$ where

$$\mathcal{H}_0/\hbar = \omega_1 \frac{\sigma_{1z}}{2} + \omega_2 \frac{\sigma_{2z}}{2} \tag{A.57}$$

and

$$\mathcal{H}_1/\hbar = \omega_{12} \frac{\sigma_{1x}\sigma_{2x} + \sigma_{1y}\sigma_{2y} + \sigma_{1z}\sigma_{2z}}{4}. \tag{A.58}$$

First-order perturbation theory says that the eigenstates are unaffected by the coupling, and the eigenvalues are changed by the diagonal matrix elements of the perturbation,

that is just the z terms. Thus to first order the Heisenberg coupling can be replaced by an Ising coupling. To check that this approach is valid we need the first-order effect on the eigenvectors, and in general the other states get mixed in according to

$$a_k^{(1)} = \frac{\langle k|\mathcal{H}_1|m\rangle}{E_m - E_k}. \tag{A.59}$$

The only off-diagonal elements in the perturbation connect the two central states; these are of size $\frac{1}{2}\,\omega_{12}$ and so mixing is negligible if

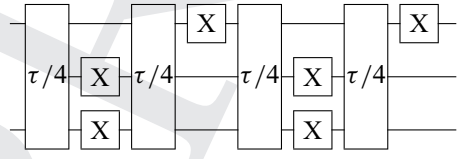
$$\left|\frac{\omega_{12}}{\omega_1 - \omega_2}\right| \ll 1. \tag{A.60}$$

An alternative approach is to diagonalize the full Hamiltonian and then take appropriate limits to show that the eigenvalues can be approximated by the diagonal elements.

3. As in the previous chapter the critical step is to make a standard controlled-Z gate, as this can be converted to a controlled-NOT gate with a couple of Hadamard gates. Now the controlled-Z can be decomposed (up to an irrelevant global phase) as evolution under the Ising coupling for a time $\tau = \pi/\omega_{12}$ together with a -90_z rotation on both qubits. The Ising term can be implemented with a spin echo as shown in equation (11.12). It might be argued that the -90_z gates are not standard, but these can be replaced by a sequence of three S gates, where $\mathrm{S} = \sqrt{\mathrm{Z}}$ is a standard gate. For a NOT gate that takes the same length of time, start from a spin echo which refocuses everything, and put a NOT gate on the beginning or end; if you are careful this NOT gate will cancel an earlier one.
4. Assuming the couplings take the Ising form, the Hamiltonian is

$$\mathcal{H}/\hbar = \tfrac{1}{2}\left(\omega_1\sigma_{1z} + \omega_2\sigma_{2z} + \omega_3\sigma_{3z}\right) + \tfrac{1}{4}\left(\omega_{12}\sigma_{1z}\sigma_{2z} + \omega_{13}\sigma_{1z}\sigma_{3z} + \omega_{23}\sigma_{2z}\sigma_{3z}\right). \tag{A.61}$$

A possible spin-echo network is



(A.62)

5. To reduce an apparent Larmor frequency, combine a period of free precession with a period under a spin echo. To change the sign of a Larmor frequency, surround a period of free precession with NOT gates. Any single component of a Hamiltonian, including couplings, can be rescaled in the range ± 1, but simultaneously rescaling multiple elements gets complicated and is not always possible.

Part III: Quantum communication

13. Basics of information theory

1. The number of substrings to be encoded is the sum of all substrings $N_s = N_{AA} + N_{AB} + N_B$ and to be consistent with the average number of messages A and B we must also have

$pN_o = 2N_{AA} + N_{AB}$ and $(1-p)N_o = N_{AB} + N_B$. A substring AB in the original message will be encoded as 10 whenever it is part of a sequence of messages of the form $BA \ldots AB$ with an odd number $2n+1$ of As. The probability for such a sequence is $(1-p)^2 p^{2n+1}$ and we therefore obtain the overall average number of encodings of a substring AB as

$$N_{AB} = N_o(1-p)^2 p \sum_{n=0}^{\infty} p^{2n} = \frac{N_o p(1-p)}{1+p}.$$

The values for N_{AA} and N_B and N_o immediately follow, and the probabilities then follow as $p_{AA} = N_{AA}/N_s$, $p_{AB} = N_{AB}/N_s$, and $p_B = N_B/N_s$.

2. We use $p_C = 1 - p_A - p_B$ and maximizing the Shannon entropy gives $p_A = p_B = p_C = 1/3$. Its maximum is given by $H(X) = \log_2(3)$ bits.
3. One message contains $H(X) = 7/4$ bits of information. We choose: $A = 0$, $B = 10$, $C = 110$, and $D = 111$. The average message length is $7/4$ and the encoding is thus optimal. Each first bit of a message encoding has probabilities $p_0 = p_A = 1/2$ and $p_1 = p_B + p_C + p_D = 1/2$. The message is encoded with at least two bits with probability $1/2$ and the second bit has probabilities $p_0 = 2p_B = 1/2$ and $p_1 = 2(p_C + p_D) = 1/2$. With overall probability $1/4$ there is a third bit in the string which has probabilities $p_0 = 4p_C = 1/2$ and $p_1 = 4p_D = 1/2$. Each bit in the string has a probability of $1/2$ of being in states 0 and 1 as required for an optimal code.
4. One message contains $H(X) = 4\log_2(3)/3$ bits of information. This corresponds to $H(X) = 4/3$ trits found by using $\log_3$ instead of $\log_2$ when working out the entropy. We choose $A = 0$, $B = 1$, $C = 20$, $D = 21$, and $E = 22$ and find the average length of an encoded message to be $4/3$ trits, that is, this encoding is optimal. Each trit has a probability of $1/3$ of being in states 0, 1 and 2, which can be worked out similarly to Exercise 13.3.
5. The probability of having values x for X and y for Y is given by $p(x,y) = p(y|x)p(x)$ if local realism may be assumed. Furthermore,

$$\begin{aligned} H(X,Y) &= -\sum_{x,y} p(x,y)\log_2(p(x)p(y|x)) \\ &= -\sum_{x} p(x)\log_2(p(x)) - \sum_{x,y} p(x,y)\log_2(p(y|x)) \\ &= H(x) - \sum_{x,y} p(x,y)\log_2(p(y|x)) \end{aligned}$$

and therefore

$$H(Y|X) = -\sum_{x,y} p(x,y)\log_2(p(y|x)) \geq 0,$$

since $p(x,y) \geq 0$ and $-\log_2(p(y|x)) \geq 0$. The conditional entropy $H(Y|X)$ is only equal to zero if Y is a deterministic function of X, that is, $p(y|x)$ only takes on values 0 and 1.

6. The joint probabilities are $p(A,A) = p(1-\ell)$, $p(A,B) = p\ell$, $p(B,A) = (1-p)\ell$, and $p(B,B) = (1-p)(1-\ell)$. The derivative of the mutual information is given by

$$\frac{\mathrm{d}H(X:Y)}{\mathrm{d}p} = (2\ell - 1)\log_2\left(\frac{\ell + p - 2\ell p}{1 - \ell - p + 2\ell p}\right).$$

This is $\mathrm{d}H(X:Y)/\mathrm{d}p = 0$ for $p = 1/2$, consistent with the symmetry of the channel which thus works best for $p = 1/2$. The channel capacity is given by

$$C(\mathcal{N}) = \log_2(2 - 2\ell) + \ell\log_2\left(\frac{\ell}{\ell - 1}\right),$$

and takes on the value of $C(\mathcal{N}) = 1$ for $\ell = 0$ and for $\ell = 1$, showing that the channel is ideal in these limiting cases. At $\ell = 1/2$ we find $C(\mathcal{N}) = 0$, that is, no information can be transmitted in this case.

14. Quantum information

1. The reduced states are $\rho_A = \rho_B = \mathbb{1}/2$. This is the same for each Bell state because there exist local operations which turn the Bell states into each other. For instance, $\sigma_z \otimes \mathbb{1}|\Psi^+\rangle = |\Psi^-\rangle$. In any Bell state $S(\rho_{AB}) = 0$ while $S(\rho_A) = S(\rho_B) = 1$. A Bell state thus contains mutual information of $S(\rho_A : \rho_B) = 2$ and negative conditional entropy.
2. The Bell states are orthogonal and thus $p_1 = p_2 = p_3 = p_4 = 1/4$ yielding $S(\rho_{AB}) = \log_2(4) = 2$, which is the maximum possible entropy. That is, the state is the maximally mixed state $\rho_{AB} = \mathbb{I}/4$. It can therefore be written as

$$\rho_{AB} = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|)/4$$

and is not entangled. The entropies of the reduced states, which are also maximally mixed, are given by $S(\rho_A) = \log_2(2) = 1$ and $S(\rho_B) = \log_2(2) = 1$.

Repeating the calculation for $\tilde{\rho}_{AB}$ gives

$$\begin{aligned}\tilde{\rho}_{AB} &= (|\psi^-\rangle\langle\psi^-| + |\phi^-\rangle\langle\phi^-|)/2 \\ &= ((|01\rangle - |10\rangle)(\langle 01| - \langle 10|) + (|00\rangle + |11\rangle)(\langle 00| + \langle 11|))/4\end{aligned}$$

and therefore $S(\tilde{\rho}_{AB}) = \log_2(2) = 1$. The reduced density operators and their entropies are

$$\tilde{\rho}_A = (|0\rangle\langle 0| + |1\rangle\langle 1| + |0\rangle\langle 0| + |1\rangle\langle 1|)/4 = (|0\rangle\langle 0| + |1\rangle\langle 1|)/2, \quad S(\tilde{\rho}_A) = \log_2(2) = 1,$$

$$\tilde{\rho}_B = (|0\rangle\langle 0| + |1\rangle\langle 1| + |0\rangle\langle 0| + |1\rangle\langle 1|)/4 = (|0\rangle\langle 0| + |1\rangle\langle 1|)/2, \quad S(\tilde{\rho}_B) = \log_2(2) = 1.$$

We obtain $S(\tilde{\rho}_{AB}) = S(\tilde{\rho}_A) = S(\tilde{\rho}_B)$ and $S(\rho_A|\rho_B) = 0$, $S(\rho_A : \rho_B) = 1$, and thus cannot decide whether the state is entangled or not from the entropies.

We write the state in matrix form in the computational basis

$$\tilde{\rho}_{AB} = (|01\rangle\langle 01| + |10\rangle\langle 10| + |00\rangle\langle 00| + |11\rangle\langle 11| - |01\rangle\langle 01| - |10\rangle\langle 10| + |00\rangle\langle 11| + |11\rangle\langle 00|)/4 = \begin{pmatrix} 1/4 & 0 & 0 & 1/4 \\ 0 & 1/4 & -1/4 & 0 \\ 0 & -1/4 & 1/4 & 0 \\ 1/4 & 0 & 0 & 1/4 \end{pmatrix}.$$

By using $|+'\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}$ and $|-'\rangle = (|0\rangle - i|1\rangle)/\sqrt{2}$ we find

$$\bar{\rho}_{AB} = (|+'-'\rangle\langle +'-'| + |-'+'\rangle\langle -'+'|)/2 = \left[\begin{pmatrix} 1 \\ i \\ i \\ 1 \end{pmatrix} \begin{pmatrix} 1 & i & -i & 1 \end{pmatrix} + \begin{pmatrix} 1 \\ i \\ -i \\ 1 \end{pmatrix} \begin{pmatrix} 1 & -i & i & 1 \end{pmatrix} \right] \frac{1}{8}$$

$$\bar{\rho}_{AB} = \begin{pmatrix} 1/4 & 0 & 0 & 1/4 \\ 0 & 1/4 & -1/4 & 0 \\ 0 & -1/4 & 1/4 & 0 \\ 1/4 & 0 & 0 & 1/4 \end{pmatrix} = \tilde{\rho}_{AB}.$$

The state is thus an incoherent mixture of two product states and not entangled.

Remark: Calculating the partial transpose of $\tilde{\rho}_{AB}$ we find

$$\tilde{\rho}_{AB}^{T_B} = (|\Psi^+\rangle\langle\Psi^+| + |\Phi^-\rangle\langle\Phi^-|)/2.$$

This is a valid density operator and therefore has no negative eigenvalues, that is, the state is not entangled.

3. The density operators can be written as $\rho_A = \sum_j p_j^A |\psi_j\rangle\langle\psi_j|$ and $\rho_B = \sum_n p_n^B |\phi_n\rangle\langle\phi_n|$. The eigenvectors of the density operator are thus $|\psi_j\rangle \otimes |\phi_n\rangle$ with a probability of $p_j^A p_n^B$, where p_j^A are the eigenvalues (probabilities) of the density operator ρ_A and p_n^B are the eigenvalues of ρ_B. We can thus write $S(\rho_{AB}) = -\sum_{j,n} p_j^A p_n^B \log_2(p_j^A p_n^B) = -\sum_{j,n} p_j^A p_n^B \log_2(p_n^B) - \sum_{j,n} p_j^A p_n^B \log_2(p_j^A) = -\sum_n p_n^B \log_2(p_n^B) - \sum_j p_j^A \log_2(p_j^A) = S(\rho_A) + S(\rho_B)$.
4. If $\rho_{AB} = |\Psi_A\rangle\langle\Psi_A| \otimes |\Psi_B\rangle\langle\Psi_B|$ then $S(\rho_{AB}) = 0$, $S(\rho_A) = 0$ and also $S(\rho_B) = 0$. Thus $S(\rho_A|\rho_B) = 0$.

   If $S(\rho_A|\rho_B) \geq 0$ then

$$0 \leq S(\rho_A|\rho_B) = S(\rho_{AB}) - S(\rho_B) = -S(\rho_B) \leq 0,$$

since $S(\rho_{AB}) = 0$ for any pure state. Therefore $0 \leq -S(\rho_B) \leq 0$ and so $S(\rho_B) = 0$ and therefore ρ_B is a pure state. This means that $\rho_{AB} = \rho_A \otimes \rho_B$ and since ρ_{AB} is pure we also have a pure ρ_A. It follows that if a pure state cannot be written in this form, and thus is entangled, it must have a conditional entropy smaller than zero.
5. After undergoing both channels the state of the systems is $\rho_{AB} = \ell\,|00\rangle\langle 00| + (1-\ell)\,|\Psi^-\rangle\langle\Psi^-|$ with eigenvalues ℓ and $1-\ell$. The mutual information is thus given by $S(\rho_A : \rho_B) \approx 1.22$ for $\ell = 1/5$.

6. If distance L needs to be covered by these channels then $\ell_a = 1-\mathrm{e}^{-\gamma L}$ for the asymmetric channel while $\ell_s = 1-\mathrm{e}^{-\gamma L/2}$ for the symmetric channel. By comparing the mutual information created in each case we find that the asymmetric channel performs slightly better for $\gamma L \lessapprox 0.63$ and the symmetric channel becomes better for larger distances.

15. Quantum communication

1. The phase shift creates the state $|\Psi\rangle = (\mathrm{e}^{\mathrm{i}\phi}|ab\rangle + |ba\rangle)/\sqrt{2}$. The beam splitters transform the state according to

$$|\mathrm{in}\rangle_1 \to \frac{1}{\sqrt{2}}(|\mathrm{out}\rangle_3 + |\mathrm{out}\rangle_4) \quad \text{and} \quad |\mathrm{in}\rangle_2 \to \frac{1}{\sqrt{2}}(|\mathrm{out}\rangle_3 - |\mathrm{out}\rangle_4).$$

The state after the beam splitter is therefore

$$|\Psi\rangle = \frac{(1+\mathrm{e}^{\mathrm{i}\phi})(|A_3B_3\rangle - |A_4B_4\rangle) + (1-\mathrm{e}^{\mathrm{i}\phi})(|A_3B_4\rangle - |A_4B_3\rangle)}{\sqrt{8}}$$

and the modulus squared of the individual amplitudes yields the probabilities for coincidence clicks in the corresponding detectors. These are $p_{A_3,B_3} = p_{A_4,B_4} = \cos^2(\phi/2)/2$ and $p_{A_3,B_4} = p_{A_4,B_3} = \sin^2(\phi/2)/2$. No other coincidences will be detected in an ideal experiment.

2. In an individual run the state after the phase shifter is $|\Psi\rangle = (\mathrm{e}^{\mathrm{i}(\phi+\varphi)}|ab\rangle + |ba\rangle)/\sqrt{2}$ and we now need to average over all possible values for the unknown phase, which is equally distributed in $[0, 2\pi[$ to obtain the density matrix

$$\rho = \frac{1}{2}\int_0^{2\pi} \mathrm{d}\varphi(\mathrm{e}^{\mathrm{i}(\phi+\varphi)}|ab\rangle + |ba\rangle)(\mathrm{e}^{-\mathrm{i}(\phi+\varphi)}\langle ab| + \langle ba|) = \frac{1}{2}(|ab\rangle\langle ab| + |ba\rangle\langle ba|).$$

This is independent of the phase shift ϕ.

3. The beam splitters transform the density matrix ρ from Example 15.3 into

$$\begin{aligned}\rho_D = \frac{1}{4}&(|A_3B_3\rangle\langle A_3B_3| + |A_3B_4\rangle\langle A_3B_4| + |A_4B_3\rangle\langle A_4B_3| + |A_4B_4\rangle\langle A_4B_4| \\ &- (|A_3B_4\rangle\langle A_4B_3| + |A_3B_3\rangle\langle A_4B_4| + \mathrm{h.c.}),\end{aligned} \tag{A.63}$$

where h.c. denotes the Hermitian conjugate of the first terms in the bracket. We therefore obtain $p_{A_3,B_3} = p_{A_4,B_4} = 1/4$ and $p_{A_3,B_4} = p_{A_4,B_3} = 1/4$ and again no other coincidences will be detected in an ideal experiment.

4. We first continue from Example 15.1 by considering the case of a symmetric spatial wavefunction $(|ul\rangle + |lu\rangle)/\sqrt{2}$. The BS turns the wavefunction into

$$\frac{(|u\rangle + |l\rangle)(|u\rangle - |l\rangle) + (|u\rangle - |l\rangle)(|u\rangle + |l\rangle)}{\sqrt{8}} = \frac{|uu\rangle - |ll\rangle}{\sqrt{2}}.$$

Both photons thus follow the same path after the BS.

The overall state containing spatial and polarization degrees of freedom must be symmetric and so the Bell states are written as

$$|\Psi^-\rangle = \frac{1}{2}(|HV\rangle - |VH\rangle)(|ul\rangle - |lu\rangle) \qquad |\Psi^+\rangle = \frac{1}{2}(|HV\rangle + |VH\rangle)(|ul\rangle + |lu\rangle),$$

$$|\Phi^-\rangle = \frac{1}{2}(|HH\rangle - |VV\rangle)(|ul\rangle + |lu\rangle) \qquad |\Phi^+\rangle = \frac{1}{2}(|HH\rangle + |VV\rangle)(|ul\rangle + |lu\rangle).$$

The photons must thus follow the same arms for all Bell states except $|\Psi^-\rangle$. Clicks in two different arms thus indicate state $|\Psi^-\rangle$, while clicks in two detectors of the same arm are caused by $|\Psi^+\rangle$. If only one detector clicks[1] then either of the states $|\Phi^\pm\rangle$ was measured. These two cannot be distinguished.

If photons were fermions the Bell states would be

$$|\Psi^-\rangle = \frac{1}{2}(|HV\rangle - |VH\rangle)(|ul\rangle + |lu\rangle) \qquad |\Psi^+\rangle = \frac{1}{2}(|HV\rangle + |VH\rangle)(|ul\rangle - |lu\rangle),$$

$$|\Phi^-\rangle = \frac{1}{2}(|HH\rangle - |VV\rangle)(|ul\rangle - |lu\rangle) \qquad |\Phi^+\rangle = \frac{1}{2}(|HH\rangle + |VV\rangle)(|ul\rangle - |lu\rangle).$$

The same arguments as above apply and again lead to the conclusion that $|\Psi^-\rangle$ and $|\Psi^+\rangle$ can be identified while $|\Phi^\pm\rangle$ are not distinguishable.

5. Four messages A, B, C, and D can faithfully be transmitted in one use of the channel with the highest mutual information achieved when they are chosen with probability $1/4$ each, giving joint probabilities of $p(A, A) = p(B, B) = p(C, C) = p(D, D) = 1/4$ and thus $C(\mathcal{N}) = 2$ bits.

   For an imperfect Bell state analyzer only three messages can be encoded. The channel capacity is thus $C(\mathcal{N}) = \log_2(3) = 1.58$ bits.
6. Follow the descriptions of these schemes in the main text with the appropriate replacements for the Bell states.
7. From Example 15.2 we know that before classical communication the state of Bob's qubit is

$$\rho_3 = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right).$$

   This is maximally mixed and does not depend on α or β. No information about the state is known to Bob before the measurement outcome is revealed.

   The initial state is unknown to Alice and she only possesses one copy of the qubit. Alice has no way of measuring the state of her qubit since any such attempt would inevitably project the qubit into an eigenstate of the measured operator and hence destroy the original state.
8. For states $|\Phi^\pm\rangle$ Bob will apply the unitary operation intended for $|\Phi^\mp\rangle$ with probability $1/2$. In these error cases Bob's operation converts his qubit into state $|\psi_E\rangle = \alpha|0\rangle - \beta|1\rangle$. After Bob has applied his unitary operation the overall state is

$$\begin{aligned}\tilde{\rho}_{123} \;=\; & (|\phi^+\rangle\langle\phi^+|/8 + |\phi^-\rangle\langle\phi^-|/8 + |\psi^-\rangle\langle\psi^-|/4 + |\psi^+\rangle\langle\psi^+|/4) \otimes |\psi\rangle\langle\psi| \\ & + (|\phi^+\rangle\langle\phi^+| + |\phi^-\rangle\langle\phi^-|) \otimes |\psi_E\rangle\langle\psi_E|/8\,.\end{aligned}$$

   We can now again trace over particles 1, 2 yielding $\tilde{\rho}_1 = 3|\psi\rangle\langle\psi|/4 + |\psi_E\rangle\langle\psi_E|/4$. The resulting fidelity with the original state is

$$F = \langle\psi|\tilde{\rho}_1|\psi\rangle = 3/4 + 1/4|\langle\psi_E|\psi\rangle|^2 = 3/4 + |1 - 2|\beta|^2|/4,$$

   with a maximum value of $F_{\max} = 1$ for $|\beta|^2 = 0$ or $|\beta|^2 = 1$, that is, states on the north and south pole of the Bloch sphere, $|\psi\rangle = |0\rangle$ or $|\psi\rangle = |1\rangle$. The minimum value $F_{\min} = 3/4$

[1] Two clicks in the case of photon number-resolving detectors.

is obtained for $|\beta|^2 = 1/2$, which are all the states on the equator of the Bloch sphere $|\psi\rangle = (|0\rangle + e^{i\phi}|1\rangle)/\sqrt{2}$ with arbitrary phase $\phi \in [0, 2\pi[$.

Remark: One may argue that the imperfect beam splitter does not project into Bell states $|\Phi^{\pm}\rangle$ but rather into states $|00\rangle$ and $|11\rangle$. In this case the density operator after Bob's operation is then

$$\tilde{\rho}_{123} = \frac{1}{4}|\psi\rangle\langle\psi|\left(\left|\Psi^-\right\rangle\left\langle\Psi^-\right| + \left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \frac{1}{2}(|\alpha|^2|000\rangle\langle 000| + |\beta|^2|111\rangle\langle 111|\right.\right.\,.$$

After tracing out particles 2 and 3 we obtain $\rho_1 = \frac{1}{2}|\psi\rangle\langle\psi| + \frac{|\alpha|^2}{2}|0\rangle\langle 0| + \frac{|\beta|^2}{2}|1\rangle\langle 1|$. Both states are identical to the ones written down above, as can easily be checked by writing them out in the computational basis.

9. This question is solved by carrying out the calculations about teleportation in the main text, making the replacements $\alpha \to |\phi\rangle_4/\sqrt{2}$ and $\beta \to |\varphi\rangle_4/\sqrt{2}$. The calculation also works for mixed-density operators.

16. Violating EPR

1. The observable $QS = -\sigma_z^{(1)}(\sigma_z^{(2)} + \sigma_x^{(2)})/\sqrt{2}$ has an expectation value given by

$$\langle QS\rangle = \langle\Psi^-|QS|\Psi^-\rangle = -(\langle 01|\sigma_z^{(1)}\sigma_z^{(2)}|01\rangle + \langle 10|\sigma_z^{(1)}\sigma_z^{(2)}|10\rangle)/\sqrt{8} = 1/\sqrt{2}.$$

Similarly for $RS = -\sigma_x^{(1)}(\sigma_z^{(2)} + \sigma_x^{(2)})/\sqrt{2}$ we find

$$\langle RS\rangle = \langle\Psi^-|RS|\Psi^-\rangle = (\langle 01|\sigma_x^{(1)}\sigma_x^{(2)}|10\rangle + \langle 10|\sigma_x^{(1)}\sigma_x^{(2)}|01\rangle)/\sqrt{8} = 1/\sqrt{2}.$$

Also, for $RT = \sigma_x^{(1)}(\sigma_z^{(2)} - \sigma_x^{(2)})/\sqrt{2}$,

$$\langle RT\rangle = \langle\Psi^-|RT|\Psi^-\rangle = (\langle 01|\sigma_x^{(1)}\sigma_x^{(2)}|10\rangle + \langle 10|\sigma_x^{(1)}\sigma_x^{(2)}|01\rangle)/\sqrt{8} = 1/\sqrt{2}.$$

and for $QT = \sigma_z^{(1)}(\sigma_z^{(2)} - \sigma_x^{(2)})/\sqrt{2}$,

$$\langle QT\rangle = \langle\Psi^-|QT|\Psi^-\rangle = -(\langle 01|\sigma_z^{(1)}\sigma_z^{(2)}|01\rangle + \langle 10|\sigma_z^{(1)}\sigma_z^{(2)}|10\rangle)/\sqrt{8} = -1/\sqrt{2}.$$

Therefore we get a violation of the CHSH inequality $\langle QS\rangle + \langle RT\rangle + \langle RS\rangle - \langle QT\rangle \leq 2$.

2. The state $|\psi^-\rangle$ is obtained from $|\phi^-\rangle$ by applying the operator $\sigma_x^{(2)}$ and thus Alice may measure the same observables Q and R while Bob should measure $S' = \sigma_x^{(2)}S\sigma_x^{(2)} = T$ and $T' = \sigma_x^{(2)}T\sigma_x^{(2)} = S$, that is, S and T change their roles.
3. As usual we identify $|H\rangle$ and $|V\rangle$ with $|0\rangle$ and $|1\rangle$ in the Z basis and then denote the corresponding basis states in the X basis by $|H'\rangle$ and $|V'\rangle$ and in the Y basis by $|R\rangle$ and $|L\rangle$. Using $\sqrt{2}|H'\rangle = |H\rangle + |V\rangle$, $\sqrt{2}|V'\rangle = |H\rangle - |V\rangle$ and $\sqrt{2}|R'\rangle = |H\rangle + i|V\rangle$,

$\sqrt{2}|L\rangle = |H\rangle - i|V\rangle$ we find

$$\begin{aligned}\frac{1}{\sqrt{2}}(|HHH\rangle + |VVV\rangle) &= \frac{1}{4}(|(H'+V')(R+L)(R+L)\rangle \\ &\quad -|(H'-V')(L-R)(L-R)\rangle) \\ &= \frac{1}{4}(|H'RR\rangle + |H'RL\rangle + |H'LR\rangle + |H'LL\rangle \\ &\quad + |V'RR\rangle + |V'RL\rangle + |V'LR\rangle + |V'LL\rangle \\ &\quad - |H'RR\rangle + |H'RL\rangle + |H'LR\rangle - |H'LL\rangle \\ &\quad + |V'RR\rangle - |V'RL\rangle - |V'LR\rangle + |V'LL\rangle) \\ &= \frac{1}{2}(|H'RL\rangle + |H'LR\rangle + |V'LL\rangle + |V'RR\rangle),\end{aligned}$$

and by symmetry we find in the other bases

$$\frac{1}{\sqrt{2}}(|HHH\rangle + |VVV\rangle) = \frac{1}{2}(|RH'L\rangle + |LH'R\rangle + |LV'L\rangle + |RV'R\rangle),$$

$$\frac{1}{\sqrt{2}}(|HHH\rangle + |VVV\rangle) = \frac{1}{2}(|RLH'\rangle + |LRH'\rangle + |LLV'\rangle + |RRV'\rangle).$$

Therefore, measuring two photons in circular R, L polarization the state of the third photon is fixed; if the two results are identical (RR or LL) then the third photon is in state V' and for opposite polarizations (LR or RL) the polarization of the third photon is H'. Let us consider a measurement in the XXX basis. Quantum mechanically we find

$$\begin{aligned}\frac{1}{\sqrt{2}}(|HHH\rangle + |VVV\rangle) &= \frac{1}{4}(|(H'+V')(H'+V')(H'+V')\rangle \\ &\quad +|(H'-V')(H'-V')(H'-V')\rangle) \\ &= \frac{1}{2}(|H'H'H'\rangle + |H'V'V'\rangle + |V'H'V'\rangle + |V'V'H'\rangle).\end{aligned}$$

Which outcomes are possible if the polarizations are elements of reality? The permutations of $|\mathrm{GHZ}\rangle$ above imply that if H (V) is obtained for one photon, the other two have to have opposite (identical) circular polarization. Imagine we find V and V for photons 2 and 3. Since 3 is V, 1 and 2 have to have identical circular polarization. Also, since 2 is V, 1 and 3 have to have identical circular polarization. If all of these are elements of reality, then all photons have identical circular polarization. Thus photon 1 needs to carry polarization V. We conclude that $|VVV\rangle$ is a possible outcome. Similarly, one can verify that the only four possible outcomes are

$$|V'V'V'\rangle \qquad |H'H'V'\rangle \qquad |H'V'H'\rangle \qquad |V'H'H'\rangle.$$

Local realism and quantum mechanics predict opposite results in all cases!

4. In order to answer this question we need to follow Example 16.3. We find that $1/2$ of the events will not lead to the right number of clicks in T. Another factor of $1/2$ comes from requiring a single click in D_3 and the final stage of the analysis gives another factor of $1/2$. Therefore we overall find that the probability is $1/8$. Combining

this with the requirement to produce two entangled pairs, the overall probability is $p = 10^{-6}/8 = 1.25 \times 10^{-7}$.

17. Quantum cryptography

1. (a) Alice and Bob will choose the matching bases for 50% of the qubits. This gives a key generation rate of 500 bits per second on average.

   (b) If an eavesdropper is present the number of intercepted qubits n to be compared for detecting Eve with probability P is $n = \log_2(1-P)/\log_2(p_r)$, where p_r is the probability of Eve not affecting the bit value. Eve intercepts each bit with probability $1/2$ and changes intercepted bits with probability $1/4$. This leads to a probability of $p_r = 7/8$ for a bit compared by Alice and Bob to not be affected by the presence of Eve, and thus $n_{\text{compare}} = \log_2(1-P)/\log_2(7/8) = 51.7 \approx 52$.

   Out of the key of 1000 bits established in two seconds, Alice and Bob need to sacrifice $n_{\text{compare}} = 52$ bits. This gives a key generation rate of 474 bits/sec. In two seconds Eve measured 1000 qubits. On average, 526 of them were discarded or used for comparison by Alice and Bob $\Rightarrow$ 474 bits in the key remain, each with probability $3/4$ of being correct, resulting in 89 bits of mutual information. ($H(X:Y) = 1 + 1 - 2(\log_2(8) + 3\log_2(8/3))/8) = 0.1887$.) Alice and Bob end up with 948 bits, each pair agreeing with probability $7/8$ and thus a mutual information of 433 bits ($H(X:Y) = 1 + 1 - 2(\log_2(16) + 7\log_2(16/7))/16) = 0.456$).
2. Measuring at an angle ϕ corresponds to projecting onto the states $|\phi_+\rangle = \cos(\phi)|0\rangle + \sin(\phi)|1\rangle$ with eigenvalue $+1$ and $|\phi_-\rangle = -\sin(\phi)|0\rangle + \cos(\phi)|1\rangle$ with eigenvalue -1, as shown in Example 16.2. Thus we have

$$\langle\phi_-|0\rangle = -\sin\phi \qquad \langle\phi_-|1\rangle = \cos\phi \qquad \langle\phi_+|0\rangle = \cos\phi \qquad \langle\phi_+|1\rangle = \sin\phi$$

and find for $P_{\pm,\pm} = \langle\phi_\pm, \phi_\pm|\ \Psi^-\rangle\langle\Psi^-|\ \phi_\pm, \phi_\pm\rangle$

$$P_{++}(\phi_A, \phi_B) = \frac{1}{2}(\cos(\phi_A)\sin(\phi_B) - \sin(\phi_A)\cos(\phi_B))^2 = \frac{1}{2}\sin^2(\phi_A - \phi_B),$$

$$P_{+-}(\phi_A, \phi_B) = \frac{1}{2}(\cos(\phi_A)\cos(\phi_B) + \sin(\phi_A)\sin(\phi_B))^2 = \frac{1}{2}\cos^2(\phi_A - \phi_B),$$

$$P_{-+}(\phi_A, \phi_B) = \frac{1}{2}(-\sin(\phi_A)\sin(\phi_B) - \cos(\phi_A)\cos(\phi_B))^2 = \frac{1}{2}\cos^2(\phi_A - \phi_B),$$

$$P_{--}(\phi_A, \phi_B) = \frac{1}{2}(-\sin(\phi_A)\cos(\phi_B) + \cos(\phi_A)\sin(\phi_B))^2 = \frac{1}{2}\sin^2(\phi_A - \phi_B).$$

Therefore

$$\begin{aligned} E(\phi_A, \phi_B) &= P_{++}(\phi_A, \phi_B) + P_{--}(\phi_A, \phi_B) - P_{+-}(\phi_A, \phi_B) - P_{-+}(\phi_A, \phi_B) \\ &= -\cos(2(\phi_a - \phi_b)). \end{aligned}$$

We can now compare this with a direct calculation of the expectation value:

$$E(\phi_A, \phi_B) = \langle\Psi^-|\sigma_{\phi_A} \otimes \sigma_{\phi_B}|\Psi^-\rangle = -\cos(2(\phi_a - \phi_b)).$$

3. A change in the path length (which is much shorter than the coherence length and thus keeps the spatial overlap of the photons at the beam splitter close to one) results in a phase shift that adds directly to ϕ_A. The detector which should ideally not click will now click with probability $\sin^2(\Delta\phi)$, and the other detector with probability $\cos^2(\Delta\phi)$. Averaging over the equally distributed phases we find, for the probability Δp of a click in the wrong detector,

$$\Delta p = \int_{-\pi/20}^{\pi/20} \mathrm{d}\Delta\phi \, \sin^2(\Delta\phi) \approx 0.26\% \, .$$

4. In the setup shown in Figure 17.1(b) the operations carried out by Alice are described by

$$|0\rangle \to \frac{1}{\sqrt{2}} \left(|0, \Delta\rangle + \mathrm{e}^{\mathrm{i}\phi_A} |1\rangle \right) \to \frac{1}{2} \left(|0, \Delta\rangle + |1, \Delta\rangle + \mathrm{e}^{\mathrm{i}\phi_A} (|0\rangle - |1\rangle) \right) .$$

Here Δ denotes a delay with respect to the original mode larger than the coherence length. Only states in the lower arm ($|1\rangle$ and $|1, \Delta\rangle$) are kept. At Bob's place the state is manipulated further:

$$\begin{aligned} &\frac{1}{\sqrt{8}} \left(|0, \Delta\rangle - |1, \Delta\rangle - \mathrm{e}^{\mathrm{i}\phi_A} (|0\rangle - |1\rangle) \right) \\ &\quad \to \frac{1}{\sqrt{8}} \left(\mathrm{e}^{\mathrm{i}\phi_B} |0, \Delta\rangle - |1, 2\Delta\rangle - \mathrm{e}^{\mathrm{i}\phi_A} (|0\rangle - |1, \Delta\rangle) \right) . \end{aligned}$$

Only those terms with a delay Δ lead to interference and the others are discarded. Thus we obtain the state

$$\frac{1}{\sqrt{8}} \left(\mathrm{e}^{\mathrm{i}\phi_B} |0, \Delta\rangle + \mathrm{e}^{\mathrm{i}\phi_A} |1, \Delta\rangle \right) .$$

In this setup both pulses travel along the same fiber and variations (slow on the time scale of the delay Δ) in the phase only contribute an irrelevant global phase.

This state can be used as described in the main text for the setup in Figure 17.1(a) to realize the BB84 protocol. Note the normalization of the state, which indicates that this protocol only succeeds 1/4 of the time with single photons.