1. **Quantum circuits.** The SWAP gate performs the map $|x⟩|y⟩ \mapsto |y⟩|x⟩$ for $x, y \in \{0, 1\}$ and is denoted in a quantum circuit by $\times$.

(a) Write down the matrix corresponding to SWAP with respect to the computational basis and hence, or otherwise, show that SWAP is unitary.

**Answer sketch:** The matrix is
\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}.
\]

Multiplying this matrix by its conjugate transpose gives the identity, so SWAP is unitary.

(b) Show that, for any quantum states of one qubit $|ψ⟩, |φ⟩$, $\text{SWAP} |ψ⟩|φ⟩ = |φ⟩|ψ⟩$.

**Answer sketch:** Expand $|ψ⟩ = α|0⟩ + β|1⟩$, $|φ⟩ = γ|0⟩ + δ|1⟩$, so
\[
|ψ⟩|φ⟩ = αγ|00⟩ + αδ|01⟩ + βγ|10⟩ + βδ|11⟩,
\]
and use linearity of the SWAP gate.

(c) Consider the following quantum circuit, where $|ψ⟩, |φ⟩$ are arbitrary states of one qubit.

What is the probability that the result of measuring the first qubit is 1 in each of these two cases?

i. $|ψ⟩ = |0⟩$, $|φ⟩ = |1⟩$. **Answer sketch:** The quantum circuit performs the following sequence of operations:
\[
|0⟩|ψ⟩|φ⟩ \mapsto \frac{1}{\sqrt{2}}(|0⟩ + |1⟩)|ψ⟩|φ⟩ \mapsto \frac{1}{\sqrt{2}}(|0⟩|ψ⟩|φ⟩ + |1⟩|φ⟩|ψ⟩) \\
\mapsto \frac{1}{2} \left( |0⟩(|ψ⟩|φ⟩ + |φ⟩|ψ⟩) + |1⟩(|ψ⟩|φ⟩ − |φ⟩|ψ⟩) \right).
\]
Inserting $|\psi\rangle = |0\rangle$, $|\phi\rangle = |1\rangle$, we get that the final state before the measurement is

$$\frac{1}{2} (|0\rangle(|01\rangle + |10\rangle) + |1\rangle(|01\rangle - |10\rangle)),$$

so the probability that we see an outcome of 1 when we measure the first qubit is 1/2.

ii. $|\psi\rangle = |\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Answer sketch: By a similar calculation, the probability that we see an outcome of 1 is 0 (because $|\psi\rangle|\phi\rangle - |\phi\rangle|\psi\rangle = 0$).

2. Grover’s algorithm.

(a) Imagine we would like to solve the unstructured search problem on a set of size $N$, where we know that there are $M$ marked elements, for some $M$. Let $S$ denote the set of marked elements and write $U_f = I - 2\Pi_S$, where $\Pi_S = \sum_{x \in S} |x\rangle\langle x|$.

i. Show that $U_f^2 = I$ and hence that $U_f$ is unitary. Answer sketch: $U_f^2 = (I - 2\Pi_S)(I - 2\Pi_S) = I - 4\Pi_S + 4(\Pi_S)^2 = I - 4\Pi_S + 4\Pi_S = I$.

ii. Show that, if $M = N/4$, the unstructured problem can be solved with one use of the oracle operator $U_f$. Answer sketch: After 1 iteration, the overlap of the state of the algorithm with the uniform superposition $|S\rangle$ over elements of $S$ is $\sin^2(3\arcsin 1/2) = 1$. (This uses the argument from Secs 3-3.1 of the lecture notes, but could also be shown via direct calculation.)

(b) Imagine we apply standard Grover search for a unique marked element, but in fact every element is marked ($M = N$). Does the algorithm succeed? Why or why not? Answer sketch: Setting $U_f = -I$ in Grover’s algorithm, and noting that $D|+\rangle = |+\rangle$, the final state in the algorithm is $\pm|+\rangle$. Measuring this state gives a uniformly random outcome, so the algorithm succeeds in that it returns a marked element.

3. The QFT and periodicity.

(a) Using the formula for a geometric series, or otherwise, write down an expression for $Q_N^2$ for any $N$. Answer sketch:

$$\langle x|Q_N^2|y\rangle = \frac{1}{N} \sum_z \omega_N^{(x+y)z} = \begin{cases} 1 & \text{if } x = -y \\ 0 & \text{otherwise} \end{cases}.$$
(b) Run through the steps of the periodicity-determination algorithm for the periodic function \( f : \mathbb{Z}_4 \to \mathbb{Z}_2 \) where \( f(0) = 1, f(1) = 0, f(2) = 1, f(3) = 0 \), choosing an arbitrary measurement outcome in step 3. What is the distribution on measurement outcomes? What is the probability that the algorithm succeeds? Answer sketch: The state after step 2 of the algorithm is \[ \frac{1}{\sqrt{2}} (|0\rangle|1\rangle + |1\rangle|0\rangle + |2\rangle|1\rangle + |3\rangle|0\rangle). \] Imagine we get measurement outcome 0. Then the state collapses to \[ \frac{1}{\sqrt{2}} (|1\rangle|0\rangle + |3\rangle|0\rangle). \] After applying the QFT, the resulting state of the first register is \[ \frac{1}{\sqrt{2}} (|0\rangle - |2\rangle), \] so the distribution on measurement outcomes is uniform on outcomes 0 and 2. In the second case, we cancel down the fraction 2/4 to 1/2 and output a period of 2; in the first case, the algorithm fails. So it succeeds with probability 1/2.

4. Shor's algorithm.

(a) Assume that we would like to factorise \( N = 33 \) and pick \( a = 10 \). Determine the order of \( a \) mod \( N \) and hence factorise \( N \). Answer sketch: \( 10^2 = 100 \equiv 1 \) mod 33, so the order \( r \) of \( a \) mod \( N \) is 2. Following the integer factorisation algorithm, we compute \( \gcd(a^{r/2} - 1, N) = \gcd(9, 33) = 3 \). We output 3 as a factor of 33.

(b) Write down the continued fraction expansion of \( \frac{17}{32} \) and the corresponding sequence of convergents. Answer sketch:

\[
\frac{17}{32} = \frac{1}{2} = \frac{1}{1 + \frac{15}{32}} = \frac{1}{1 + \frac{1}{\frac{32}{15}}} = \frac{1}{1 + \frac{1}{1 + \frac{1}{\frac{16}{5}}}} = \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}},
\]

The sequence of convergents is thus

\[
\frac{1}{1}, \quad \frac{1}{1 + \frac{1}{1}} = \frac{2}{3}, \quad \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}} = \frac{8}{15}.
\]

(c) Describe all the ways that Shor’s algorithm can fail to factorise an integer \( N \). Answer sketch: Shor’s algorithm fails if: the order \( r \) of the randomly chosen value of \( a \) mod \( N \) is odd; or \( a^{r/2} - 1 \) and \( N \) are coprime; or the measurement result at the end of the quantum algorithm is not “good”, i.e. the closest integer to \( M/r \), where \( M \) is the smallest power of 2 larger than \( N^2 \).

5. Phase estimation and Hamiltonian simulation.

(a) Write down the full quantum circuit for phase estimation with \( n = 3 \) (but not
decomposing the inverse quantum Fourier transform). **Answer sketch:**

![Diagram of quantum circuit](image)

(b) What is the minimal $k$ such that the Hamiltonian $H = 2X \otimes X \otimes I - 3Z \otimes I \otimes Z$ is $k$-local? What is the minimal $k$ such that $H^2$ is $k$-local? **Answer sketch:** $H$ is 2-local but not 1-local. $H^2 = 13 I \otimes I \otimes I$, which is 0-local.

(c) Let $H$ be a Hamiltonian on $n$ qubits, and imagine we can produce a state $|\psi\rangle$ such that $|\psi\rangle$ is an eigenvector of $H$ with eigenvalue $\lambda$. Describe how phase estimation can be combined with Hamiltonian simulation to approximately determine $\lambda$. **Answer sketch:** Hamiltonian simulation allows us to approximately implement the unitary operator $U(t) = e^{-iHt}$, for any $t$. Then $|\psi\rangle$ is an eigenvector of $U(t)$ with eigenvalue $e^{-i\lambda t}$. Applying phase estimation to $U(t)$ allows us to approximately determine $\lambda t$, and hence $\lambda$. To be more precise, this only allows us to determine $\lambda t \mod 2\pi$ (why?). It is sufficient to choose $t = O(1/\lambda_{\text{max}})$, where $\lambda_{\text{max}}$ is an upper bound on $|\lambda|$, for this to imply a reasonable estimate of $\lambda$.

6. Noise, quantum channels and error-correction.

(a) The phase-damping channel $E_P$ is described by Kraus operators

$$E_0 = \sqrt{1-p} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad E_1 = \begin{pmatrix} \sqrt{p} & 0 \\ 0 & 0 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{p} \end{pmatrix}$$

for some $p$ such that $0 \leq p \leq 1$.

i. What is the result of applying $E_P$ to a mixed state $\rho$ of the form

$$\rho = \begin{pmatrix} \alpha & \beta \\ \beta^* & \gamma \end{pmatrix}$$

in the computational basis? **Answer sketch:**

$$\rho = \begin{pmatrix} \alpha & (1-p)\beta \\ (1-p)\beta^* & \gamma \end{pmatrix}$$
ii. Determine the representation of $\mathcal{E}_P$ as an affine map $v \mapsto Av + b$ on the Bloch sphere. **Answer sketch:** We compute the effect of $\mathcal{E}_P$ on $I/2$ and Pauli matrices,

$$\mathcal{E}_P(I/2) = I/2, \quad \mathcal{E}_P(X) = (1 - p)X, \quad \mathcal{E}_P(Y) = (1 - p)Y, \quad \mathcal{E}_P(Z) = Z.$$ 

So $b = (0, 0, 0)^T$ and

$$A = \begin{pmatrix} 1 - p & 0 & 0 \\ 0 & 1 - p & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$ 

(b) Imagine we encode the state $\alpha|0\rangle + \beta|1\rangle$ using the bit-flip code (i.e. $|0\rangle \mapsto |000\rangle$ and $|1\rangle \mapsto |111\rangle$) and a $Y$ error occurs on the second qubit. What is the decoded state? **Answer sketch:** We can compute explicitly that the effect of the error on the encoded state $\alpha|000\rangle + \beta|111\rangle$ is to produce the state $\alpha i|010\rangle - \beta i|101\rangle$. The error-correction procedure flips the incorrect second bit to produce $\alpha i|000\rangle - \beta i|111\rangle$. So the final decoded state is $\alpha i|0\rangle - i\beta|1\rangle$. (Note that the overall phase of $i$ is irrelevant.)