INTRODUCTION TO QUANTUM INFORMATION SCIENCE

Problem Sheet 3
Hilary Term

ARTUR EKERT & ZHENYU CAI

Questions Label: A - Bookwork B - Standard C - Challenging/Optional

3.1.B **Entanglement and Bell.** A source repeatedly generates two entangled qubits in the state $|\Omega\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$,

$$|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

One qubit is sent to Alice and one to Bob.

(1) When Alice measures her qubit in the standard Z basis, she *instantaneously* knows whether Bob, who may be miles away, will observe outcome 0 or 1 when he measures his qubit in the Z basis. Explain why these correlations cannot be used for instantaneous communication but they can be used for generating cryptographic keys.

(2) Show that for any two operators $A, B \in \mathcal{B}(\mathbb{C}^2)$, we have

$$\langle\Omega|\, A \otimes B\, |\Omega\rangle = \frac{1}{2}\operatorname{tr} A^T B.$$

(3) Let A and B be two observables measured by Alice and Bob, respectively,

$$A = \cos\alpha Z + \sin\alpha X, \quad \text{and} \quad B = \cos\beta Z + \sin\beta X, \tag{1}$$

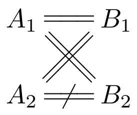
where X and Z are the Pauli operators. Show that

$$\langle\Omega|\, A \otimes B\, |\Omega\rangle = \cos(\alpha - \beta).$$

What is the probability that the results registered by Alice and Bob upon measuring these observables are identical?

Let A_1, A_2, B_1 and B_2 be the observables defined by using the angles $\alpha_1 = \frac{\pi}{2}$, $\alpha_2 = 0$, $\beta_1 = \frac{\pi}{4}$ and $\beta_2 = \frac{3\pi}{4}$ (respectively) in Eq. (1). Alice and Bob perform a statistical test (known as the CHSH test) in which Alice repeatedly measures either A_1 or A_2, and Bob either B_1 or B_2. For each run they choose, randomly and independently from each other, which observable to measure, and then check whether the following conditions are satisfied:

$$A_1 = B_1, \quad A_1 = B_2, \quad A_2 = B_1, \quad A_2 \neq B_2. \tag{2}$$



In each run they are able to check only *one* of the four conditions depending on the pair of observables they choose to measure.

(4) Show that their probability P_s of success (i.e. the asymptotic fraction of runs in which they find that the outcomes agree with the conditions in Eq. (2)) is given by $P_s = \cos^2\frac{\pi}{8}$.

The CHSH test described above can be performed using two devices, $\mathcal{A}$ and $\mathcal{B}$, with $\mathcal{A}$ being a "black box" of unknown design that has two settings A_1 and A_2, and similarly for $\mathcal{B}$ with the settings being B_1 and B_2. At each run of the device $\mathcal{A}$ or $\mathcal{B}$ for a given setting, an outcome of ±1 is generated. The probability of success in any such CHSH test cannot exceed $P_s = \cos^2\frac{\pi}{8}$. The maximum value is achieved only when the settings correspond to the measurements on qubits in state $|\Omega\rangle$, as described above (modulo some simple relabelling). The test is rigid — there is no other way to maximise the probability of success.

(5) An adversary, Eve, who manufactured, pre-programmed, and sold the two devices to Alice and Bob, claims that for each run of the CHSH test she has assigned numerical values ±1 to A_1, A_2, B_1, and B_2 so that the outcomes are predetermined. Alice and Bob run the CHSH test using their unreliable devices and obtain $P_s \approx 0.85$. Is the claim from Eve true?

(6) Would the CHSH test be conclusive if Alice and Bob, in their "random" choices of measurements (A_1 or A_2 for Alice, and B_1 or B_2 for Bob), relied on random number generators supplied by their adversary Eve?

Solution: See Chapter 9 of the online book and Lecture 5.9.

(1) No instantaneous communication since Alice and Bob cannot control the measurement outcome, i.e. the outcome is random to each of them.

However, this randomness is shared between Alice and Bob, and such a shared randomness can be used to generate shared cryptographic keys for encoding and decoding messages to achieve secure classical communication.

(2)

$$|\Omega\rangle = \frac{1}{\sqrt{2}} \sum_{i=0}^{1} |ii\rangle$$

$$\begin{aligned}\langle\Omega| A \otimes B |\Omega\rangle &= \frac{1}{2} \sum_{i,j=0}^{1} \langle jj| A \otimes B |ii\rangle = \frac{1}{2} \sum_{i,j=0}^{1} \langle j| A |i\rangle \langle j| B |i\rangle \\ &= \frac{1}{2} \sum_{i,j=0}^{1} A_{ij}^{T} B_{ji} = \frac{1}{2} \mathrm{Tr}\left(A^T B\right)\end{aligned}$$

Note that it is A^T not $A^\dagger$.

(3) Z and X are both symmetric: $Z^T = Z$, $X^T = X$.

$$\langle\Omega| A \otimes B |\Omega\rangle = \frac{1}{2} \mathrm{Tr}\left(A^T B\right)$$

$$= \frac{1}{2} \mathrm{Tr}[(\cos\alpha Z + \sin\alpha X)\,(\cos\beta Z + \sin\beta X)]$$

$$= \frac{1}{2} \mathrm{Tr}[\cos\alpha\cos\beta \mathbb{1} + \sin\alpha\sin\beta\mathbb{1} + \cos\alpha\sin\beta ZX + \sin\alpha\cos\beta XZ]$$

Using $\mathrm{Tr}(\mathbb{1}) = 2$ and $\mathrm{Tr}(XZ) = \mathrm{Tr}(ZX) = 0$, we have:

$$\langle\Omega| A \otimes B |\Omega\rangle = \cos\alpha\cos\beta + \sin\alpha\sin\beta = \cos(\alpha - \beta)$$

Since $A^2 = \mathbb{1}$ and $\mathrm{Tr}(A) = 0$, we know that the eigenvalue of A is ± 1 and similarly for B (can also obtain their eigenvalues via direct calculation). Hence, $A \otimes B$ is an observable that will take the value $+1$ when the measurement outcomes of A and B are the same and -1 otherwise. Given the state $|\Omega\rangle$, denoting the probability of the observable $A \otimes B$ takes the value ± 1 as $P_{\pm 1}$, we have $P_{+1} + P_{-1} = 1$ and

We can also make use of the fact that $A = Ze^{i\alpha Y} = e^{-i\frac{\alpha}{2}Y} Z e^{i\frac{\alpha}{2}Y}$ i.e. the observable A is simply the observable Z transform by an α-rotation around the Y axis in the Bloch sphere. Similarly, we have: $B = Ze^{i\beta Y} = e^{-i\frac{\beta}{2}Y} Z e^{i\frac{\beta}{2}Y}$

$$\begin{aligned}\langle\Omega| A \otimes B |\Omega\rangle = (+1) \times P_{+1} + (-1) \times P_{-1} &= \cos(\alpha - \beta) \\ P_{+1} - (1 - P_{+1}) &= \cos(\alpha - \beta)\end{aligned}$$

Hence,

$$P_{+1} = \frac{\cos(\alpha - \beta) + 1}{2} = \cos^2\left(\frac{\alpha - \beta}{2}\right)$$

(4) In each run they are equally likely to choose one of the following pairs of observables to measure

$$\{A_1,\ B_1\},\quad \{A_1,\ B_2\},\quad \{A_2,\ B_1\},\quad \{A_2,\ B_2\}$$

and the condition (2) is fulfilled when the corresponding measurement outcome is:

$$A_1 \otimes B_1 = +1,\quad A_1 \otimes B_2 = +1,\quad A_2 \otimes B_1 = +1,\quad A_2 \otimes B_2 = -1.$$

Hence, the success probability is:

$$\begin{aligned} P_s &= \frac{1}{4}\left[P_{+1}(A_1, B_1) + P_{+1}(A_1, B_2) + P_{+1}(A_2, B_1) + P_{-1}(A_2, B_2)\right] \\ &= \frac{1}{4}\left[\cos^2\left(\frac{\alpha_1-\beta_1}{2}\right) + \cos^2\left(\frac{\alpha_1-\beta_2}{2}\right) + \cos^2\left(\frac{\alpha_2-\beta_1}{2}\right) + \sin^2\left(\frac{\alpha_2-\beta_2}{2}\right)\right] \\ &= \frac{1}{4}\left[\cos^2\left(\frac{\pi}{8}\right) + \cos^2\left(\frac{\pi}{8}\right) + \cos^2\left(\frac{\pi}{8}\right) + \underbrace{\sin^2\left(\frac{3\pi}{8}\right)}_{\cos^2\left(\frac{\pi}{8}\right)}\right] \\ &= \cos^2\left(\frac{\pi}{8}\right) \end{aligned}$$

(5) If we assigned a set of values (±1) for our four variable $\{A_1,\ A_2,\ B_1,\ B_2\}$, then at least one of the four conditions in Eq. (2) will be violated. Thus as we randomly choose one possible pair of observables to measure, which is effectively randomly selecting one of the four conditions in Eq. (2) to check if it is satisfied, we will only have at most 3/4 success probability:

$$P_s = \frac{3}{4}.$$

Since $P_s \approx 0.85 \approx \cos^2(\frac{\pi}{8})$, we know that Eve has no knowledge about the values of the observables prior to their measurement, and the measurement results from the devices should be generated from genuine quantum measurement of the observables on the entangled qubits in the state $|\Omega\rangle$.

(6) In this way, Eve essentially control the probability distribution of choosing which pair of observables $\{A_i, B_j\}$ to measure and thus which one of the four conditions in Eq. (2) will be checked. In this way, if Eve assign a set of predetermined values to the observable, she can tune P_s to any value she want by simply tuning the probability of checking the violated condition in Eq. (2). Hence, the CHSH test would be meaningless in this way.

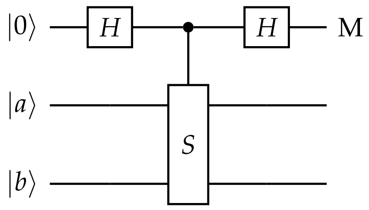
3.2.B **Playing with conditional unitaries.** The swap gate S on two qubits is defined first on product vectors, $S : |a\rangle\,|b\rangle \mapsto |b\rangle\,|a\rangle$ and then extended to sums of products vectors by linearity.

(1) Show that the four Bell states $\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $\frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ are eigenvectors of S which form the orthonormal basis in the Hilbert space associated with two qubits. Which Bell states span the symmetric subspace (all eigenvectors of S with eigenvalue 1) and which the antisymmetric one (all eigenvectors of S with eigenvalue -1)? Can S have any other eigenvalues except ±1?

(2) Show that $\Pi_\pm = \frac{1}{2}(\mathbb{1} \pm S)$ are two orthogonal projectors which form the decomposition of the identity and project on the symmetric and the antisymmetric subspaces. Decompose the state vector $|a\rangle\,|b\rangle$ of two qubits into symmetric and antisymmetric components.

An operator A is a projector iff it is idempotent: $A^2 = A$.

(3) Consider the following quantum network composed of the two Hadamard gates, one controlled-S operation (also known as the controlled-swap or the Fredkin gate) and the measurement M in the computational basis,



The state vectors $|a\rangle$ and $|b\rangle$ are normalised but not orthogonal to each other. Step through the execution of this network, writing down quantum states of the three qubits after each computational step. What are the probabilities of observing 0 or 1 when the measurement M is performed?

(4) Explain why this quantum network implements projections into the symmetric and the antisymmetric subspaces of the two qubits.

(5) Two qubits are transmitted through a quantum channel which applies the same, randomly chosen, unitary operation U to each of them. Show that $U \otimes U$ leaves the symmetric and antisymmetric subspaces invariant.

(6) Polarised photons are transmitted through an optical fibre. Due to the variation of the refractive index along the fibre the polarisation of each photon is rotated by the same unknown angle. This makes communication based on polarisation encoding unreliable. However, if you can prepare any polarisation state of two photons you can still use the channel and communicate without any errors. How can this be achieved?

Solution:

(1) Since $S^2 = I$, we know that the eigenvalue of S should satisfy $\lambda^2 = 1$, which means $\lambda = \pm 1$.

- $\lambda = +1$ (Exchange Symmetric, Triplet):

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\Psi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

- $\lambda = -1$ (Exchange Antisymmetric, Singlet)

$$|\Psi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

(2) Using

$$\Pi_\pm = \frac{I \pm S}{2}, \quad S^2 = I$$

we have:

$$\Pi_\pm^2 = \Pi_\pm \quad \text{(idempotent)}$$

Hence, $\Pi_\pm$ are projection operators. We can also show that:

$$\Pi_+ \Pi_- = 0$$

Hence, the subspaces that Π_+ and Π_- projecting into are orthogonal to each other.

Since $S\Pi_\pm = \pm\Pi_\pm$, we know that Π_+ is the projector into the exchange symmetric ($\lambda = +1$) subspace while Π_- is the projector into the exchange anti-symmetric ($\lambda = -1$) subspace.

We have $\Pi_+ + \Pi_- = I$, therefore the set of projectors $\{\Pi_+, \Pi_-\}$ formed a decomposition of the identity, i.e. the subspaces they represent span the whole Hilbert space. Hence, any state vector can be decomposed into a superposition of exchange symmetric and exchange antisymmetric components:

$$|\psi\rangle = \underbrace{\Pi_+ |\psi\rangle}_{\text{symmetric}} + \underbrace{\Pi_- |\psi\rangle}_{\text{antisymmetric}}$$

In the case of $|\psi\rangle = |ab\rangle$, we have:

$$|ab\rangle = \Pi_+ |ab\rangle + \Pi_- |ab\rangle = \underbrace{\frac{|ab\rangle + |ba\rangle}{2}}_{\text{symmetric}} + \underbrace{\frac{|ab\rangle - |ba\rangle}{2}}_{\text{antisymmetric}}$$

(3) Stepping through the circuit:

$$\begin{aligned} |0\rangle |ab\rangle &\xrightarrow{H} \propto (|0\rangle + |1\rangle) |ab\rangle \\ &\xrightarrow{\text{C-swap}} \propto |0\rangle |ab\rangle + |1\rangle |ba\rangle \\ &\xrightarrow{H} \propto (|0\rangle + |1\rangle) |ab\rangle + (|0\rangle - |1\rangle) |ba\rangle \\ &\propto |0\rangle (|ab\rangle + |ba\rangle) + |1\rangle (|ab\rangle - |ba\rangle) \end{aligned}$$

Adding in the normalisation constant, the end state is:

$$|\psi\rangle = |0\rangle \frac{|ab\rangle + |ba\rangle}{2} + |1\rangle \frac{|ab\rangle - |ba\rangle}{2} = |0\rangle \underbrace{(\Pi_+ |ab\rangle)}_{\text{symmetric}} + |1\rangle \underbrace{(\Pi_- |ab\rangle)}_{\text{antisymmetric}}$$

Here we see that measuring 0 on the first qubit will get us the symmetric component for the other two qubits, while measuring 1 will get us the antisymmetric component.

To obtain the probability of measuring 0 on the first qubit (control qubit), let us denote the projector of the first qubit into the 0 and 1 state as:

$$\Pi_0 = |0\rangle\langle 0| \otimes I, \quad \Pi_1 = |1\rangle\langle 1| \otimes I.$$

The probability of measuring 0 for the first qubit is simply the expectation value of the projector Π_0:

$$P_0 = \langle\psi| \Pi_0 |\psi\rangle = \langle ab| \Pi_+ |ab\rangle = \frac{1 + \langle ab|ba\rangle}{2} = \frac{1 + |\langle a|b\rangle|^2}{2}$$

and the corresponding output state after the measurement is simply:

$$\frac{\Pi_0 |\psi\rangle}{\sqrt{P_0}} = |0\rangle \frac{\Pi_+ |ab\rangle}{\sqrt{P_0}}.$$

Hence, the corresponding output state of the target qubits is

$$\frac{\Pi_+ |ab\rangle}{\sqrt{P_0}} = \frac{1}{2\sqrt{P_0}} (|ab\rangle + |ba\rangle)$$

which is simply the projection of $|ab\rangle$ into the exchange symmetric subspace.

Similarly, the probability of measuring 1 for the first qubit is:

$$P_1 = \langle\psi|\,\Pi_1\,|\psi\rangle = \langle ab|\,\Pi_-\,|ab\rangle = \frac{1-\langle ab|ba\rangle}{2} = \frac{1-|\langle a|b\rangle|^2}{2}$$

and the corresponding output state after the measurement is simply:

$$\frac{\Pi_1\,|\psi\rangle}{\sqrt{P_1}} = |1\rangle\,\frac{\Pi_-\,|ab\rangle}{\sqrt{P_1}}.$$

Hence, the corresponding output state of the target qubits is

$$\frac{\Pi_-\,|ab\rangle}{\sqrt{P_1}} = \frac{1}{2\sqrt{P_1}}\left(|ab\rangle - |ba\rangle\right)$$

which is simply the projection of $|ab\rangle$ into the exchange anti-symmetric subspace.

Note that such a Z measurement on the controlled qubit is equivalent to the result of directly perform S measurement on $|ab\rangle$.

(4) Discussed above.

(5) If $|\psi\rangle$ is in the $S = s$ symmetry subspace:

$$S\,|\psi\rangle = s\,|\psi\rangle\,,$$

then using the fact that $U \otimes U$ is invariant under the action of swap S: $[S, U \otimes U] = 0$, we have:

$$S\,(U \otimes U)\,|\psi\rangle = (U \otimes U)\,S\,|\psi\rangle = s\,(U \otimes U)\,|\psi\rangle$$

i.e. the state $U \otimes U\,|\psi\rangle$ is also in the $S = s$ symmetry subspace, same as $|\psi\rangle$.

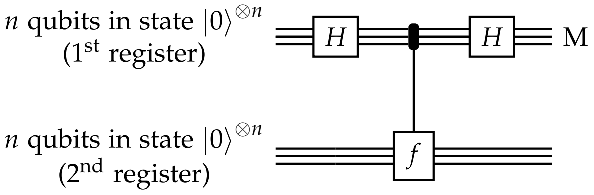
(6) We can represent one logical qubit of information using a pair of photon with the following mapping:

$$\begin{aligned} |0\rangle &\Rightarrow \frac{1}{2\sqrt{P_0}}\left(|ab\rangle + |ba\rangle\right) \\ |1\rangle &\Rightarrow \frac{1}{2\sqrt{P_1}}\left(|ab\rangle - |ba\rangle\right) \\ Z \text{ meas.} &\Rightarrow S \text{ meas.} \end{aligned}$$

As proven in (5) the measurement result of S will not be affected by random $U \otimes U$, thus our information is preserved through the noisy cable by sending through a pair of photons each time to encode one qubit of information.

3.3.A **Simon's algorithm.** Let $f : \{0,1\}^n \mapsto \{0,1\}^n$ be a 2-to-1 function such that $f(x \oplus s) = f(x)$, where s is a binary string of length n which is different from zero ($s \neq 0^n$) and $x \oplus s$ is a bit-wise addition modulo 2. In the network below the H operations denote the Hadamard transform on n qubits, M is a qubit by qubit measurement in the standard computational basis and the f operation represents a quantum evaluation of f; $|x\rangle\,|y\rangle \mapsto |x\rangle\,|y \oplus f(x)\rangle$.

Recall that the Hadamard transform is defined as $|x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}\,|y\rangle\,,$ where $x, y \in \{0,1\}^n$ and the product $x \cdot y = x_1y_1 + x_2y_2 + \ldots + x_ny_n \pmod 2$


n qubits in state $|0\rangle^{\otimes n}$
(1st register)
H
H
M
n qubits in state $|0\rangle^{\otimes n}$
(2nd register)
f

(1) What is the state of the two registers right after the quantum function evaluation?

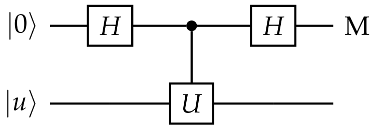
(2) The second register is measured qubit by qubit in the computational basis and a binary string $k \in \{0,1\}^n$ is registered. What is the state of the first register after the measurement?

(3) Subsequently the Hadamard transform is performed on the first register, followed by a measurement in the computational basis. The result is a binary string, z. Show that $z \cdot s = 0$.

(4) Suppose the function f is presented as an oracle. How many calls to the oracle are required in order to find s? How does it compare with a classical algorithm for the same problem? Provide rough estimates, detailed derivations are not required.

Solution: See Sec. 10.5.3 of the online book.

3.4.B **Controlled unitaries revisited.** Consider the following quantum network composed of the two Hadamard gates, one controlled-U operation and the measurement M in the computational basis,



The top horizontal line represents a qubit and the bottom one an auxiliary physical system.

(1) Suppose $|u\rangle$ is an eigenvector of U, such that $U|u\rangle = e^{i\alpha}|u\rangle$. Step through the execution of this network, writing down quantum states of the qubit and the auxiliary system after each computational step. What is the probability for the qubit to be found in state $|0\rangle$?

Regardless the state of the auxiliary system, the probability P_0 for the qubit to be found in state $|0\rangle$, when the measurement M is performed, can be written as

$$P_0 = \frac{1}{2}(1 + v\cos\phi),$$

where v and ϕ depend on U and on the initial state of the auxiliary system.

(2) Show that for an arbitrary pure state $|u\rangle$ of the auxiliary system the quantities v and ϕ are given by the relation $ve^{i\phi} = \langle u| U |u\rangle$.

(3) Suppose the auxiliary system is prepared in a mixed state described by the density operator ρ,

$$\rho = \sum_{k=1}^{n} p_k |u_k\rangle\langle u_k|$$

where vectors $|u_k\rangle$ form an orthonormal basis, $p_k \geq 0$ and $\sum_{k=1}^{n} p_k = 1$. Show that v and ϕ are given by $ve^{i\phi} = \mathrm{tr}(\rho U)$.

(4) How would you modify the network in order to estimate $\mathrm{tr}(\rho U)$? How would you estimate $\mathrm{tr}\, U$?

Solution:

(1)

$$\begin{aligned}
|0\rangle|u\rangle &\xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|u\rangle \\
&\xrightarrow{Control-U} \frac{1}{\sqrt{2}}\Big(|0\rangle|u\rangle+e^{i\alpha}|1\rangle|u\rangle\Big) \\
&= \frac{1}{\sqrt{2}}\Big(|0\rangle+e^{i\alpha}|1\rangle\Big)|u\rangle \\
&\xrightarrow{H\otimes I} \frac{1}{2}\Big[(|0\rangle+|1\rangle)+e^{i\alpha}(|0\rangle-|1\rangle)\Big]|u\rangle \\
&= \frac{1}{2}\Big[\Big(1+e^{i\alpha}\Big)|0\rangle+\Big(1-e^{i\alpha}\Big)|1\rangle\Big]|u\rangle \\
&\equiv \Big(\cos\Big(\frac{\alpha}{2}\Big)|0\rangle-i\sin\Big(\frac{\alpha}{2}\Big)|1\rangle\Big)|u\rangle
\end{aligned}$$

The control-U plus the auxiliary qubits $|u\rangle$ essentially performs $e^{-i\frac{\alpha}{2}Z}$ on the control qubit. Hence, the full circuit essentially performs $He^{-i\frac{\alpha}{2}Z}H=e^{-i\frac{\alpha}{2}X}$ on the control qubit.

The probability of measuring 0 is simply $\cos^2(\frac{\alpha}{2})$.

(2)

$$\begin{aligned}
|0\rangle|u\rangle &\xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|u\rangle \\
&\xrightarrow{Control-U} \frac{1}{\sqrt{2}}(|0\rangle|u\rangle+|1\rangle U|u\rangle) \\
&\xrightarrow{H\otimes I} \frac{1}{2}[(|0\rangle+|1\rangle)|u\rangle+(|0\rangle-|1\rangle)U|u\rangle] \\
&= \frac{1}{2}[|0\rangle(I+U)|u\rangle+|1\rangle(I-U)|u\rangle] \\
&= |\psi\rangle
\end{aligned}$$

The probability of measuring $|0\rangle$ is just the expectation value of the 0 state projector on the control qubit $\Pi_0=|0\rangle\langle 0|\otimes I$:

$$\begin{aligned}
P_0=\langle\psi|\Pi_0|\psi\rangle &= \Big(\frac{1}{2}\Big)^2\langle u|\Big(I+U^\dagger\Big)(I+U)|u\rangle \\
&= \frac{1}{4}\Big(2+\langle u|U|u\rangle+\langle u|U^\dagger|u\rangle\Big) \\
&= \frac{1+\mathrm{Re}\{\langle u|U|u\rangle\}}{2}
\end{aligned}$$

Compare to $P_0=\frac{1+v\cos\phi}{2}$, we see that $\langle u|U|u\rangle=ve^{i\phi}$.

(3) As shown in (2), using the auxiliary state $|u_k\rangle$ will measure 0 with the probability:

$$P_{0,k}=\frac{1+\mathrm{Re}\{\langle u_k|U|u_k\rangle\}}{2}.$$

When we use the set of auxiliary states $\{|u_k\rangle\}$ according to the probability distribution $\{p_k\}$, the resultant probability of measuring 0 will just be a weighted sum of $P_{0,k}$:

$$\begin{aligned} P_0 = \sum_k p_k P_{0,k} &= \frac{1+\mathrm{Re}\{\sum_k p_k \langle u_k| U |u_k\rangle\}}{2} \\ &= \frac{1+\mathrm{Re}\{\mathrm{Tr}(\sum_k p_k |u_k\rangle \langle u_k| U)\}}{2} \\ &= \frac{1+\mathrm{Re}\{\mathrm{Tr}(\rho U)\}}{2} \end{aligned}$$

Compare to $P_0 = \frac{1+v\cos\phi}{2}$, we see that $\mathrm{Tr}(\rho U) = ve^{i\phi}$.

(4) We see in (3) that we can estimate $\mathrm{Re}\{\mathrm{Tr}(\rho U)\}$ using our original circuit. In fact, if we measure the Z observable for the control qubit at the end, we have:

$$\begin{aligned} \langle Z\rangle &= (+1)\times P_0 + (-1)\times P_1 \\ &= 2P_0 - 1 \\ &= \mathrm{Re}\{\mathrm{Tr}(\rho U)\} \end{aligned}$$

If U is Hermitian, then $\mathrm{Tr}(\rho U)$ will be real: $\mathrm{Re}\{\mathrm{Tr}(\rho U)\} = \mathrm{Tr}(\rho U)$, and this will be our answer.

In the more general case in which $\mathrm{Tr}(\rho U)$ is complex, in order to obtain $\mathrm{Im}\{\mathrm{Tr}(\rho U)\}$, we will look at our original circuit from another perspective.

In our original scheme with the auxiliary qubit in the state $|u\rangle$, before the measurement we have the state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle |u\rangle + |-\rangle U |u\rangle\right).$$

If we can measure $|+\rangle\langle -|$ on the control qubit, then the expectation value is simply

$$\langle \phi| \left(|+\rangle\langle -| \otimes I\right) |\phi\rangle = \frac{1}{2}\langle u| U |u\rangle$$

which is exactly proportional to what we want.

But how do we measure $|+\rangle\langle -|$? Remember that any matrices can be decomposed into a linear sum of Pauli matrices:

$$|+\rangle\langle -| = \frac{1}{2}\left(|0\rangle\langle 0| - |1\rangle\langle 1| - |0\rangle\langle 1| + |1\rangle\langle 0|\right) = \frac{1}{2}(Z - iY)$$

Hence, the expectation value we want is simply:

$$\begin{aligned} \langle u| U |u\rangle &= 2\langle \psi| \left(|+\rangle\langle -| \otimes I\right) |\psi\rangle \\ &= \underbrace{\langle \psi| (Z\otimes I) |\psi\rangle}_{\mathrm{Re}\{\langle u|U|u\rangle\}} + i \underbrace{\langle \psi| (-Y\otimes I) |\psi\rangle)}_{\mathrm{Im}\{\langle u|U|u\rangle\}} \end{aligned}$$

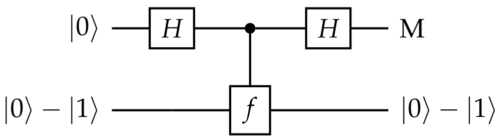
Here $\langle \psi| (Z\otimes I) |\psi\rangle$ is obtained by measuring Z on the control qubit, which can be carried out using our original circuit. It will be the real part $\mathrm{Re}\{\langle u| U |u\rangle\}$ as discussed.

Here $\langle \psi| (-Y\otimes I) |\psi\rangle)$ is obtained by measuring Y on the control qubit and multiply the result by (-1). It will be the imaginary part $\mathrm{Im}\{\langle u| U |u\rangle\}$.

Following similar arguments in (3), by using a probabilistic mixture of auxiliary states $\rho = \sum_k p_k |u_k\rangle \langle u_k|$, we can use the same circuits to obtain $\mathrm{Re}\{\mathrm{Tr}(\rho U)\}$ and $\mathrm{Im}\{\mathrm{Tr}(\rho U)\}$.

To estimate $\mathrm{Tr}(U)$, we simply set the auxiliary qubits to be in the maximally mixed state $\rho = \frac{I}{d}$ where d is the dimension of the auxiliary system.

3.5.B **Deutsch's algorithm and decoherence.** Deutsch's algorithm with an oracle $f : \{0,1\} \mapsto \{0,1\}$, is implemented by the following network



Suppose that in between the Hadamard gates the top qubit undergoes decoherence by interacting with an environment in state $|e\rangle$,

$$|0\rangle |e\rangle \mapsto |0\rangle |e_0\rangle\,, \tag{3}$$

$$|1\rangle |e\rangle \mapsto |1\rangle |e_1\rangle\,, \tag{4}$$

where $|e_0\rangle$ and $|e_1\rangle$ are the new states of the environment which are normalised but not necessarily orthogonal, $\langle e_0|e_1\rangle = v$ for some real v. How reliably can you tell whether f is constant or balanced?

Solution:

Deutsch Algorithm without Environmental Noise:

- Oracle: Some one-bit-to-one-bit function f that is either:
  (1) Constant: $f(0) = f(1)$.
  (2) Balanced: $f(0) \neq f(1)$.
- Task: Find out f is constant or balanced.

Using the oracle operation U_f with the answer bit in the state $|-\rangle$ will essentially storing the answer in the sign of the basis:

$$U_f |\vec{x}\rangle |-\rangle = (-1)^{f(\vec{x})} |\vec{x}\rangle |-\rangle$$

we see that the target qubit remained unchanged and thus we will omit the target qubit from here on and focus on only the control qubit.

The overall circuit of the Deutsch algorithm is

$$\begin{aligned} |0\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}} \sum_k |k\rangle \\ &\xrightarrow{U_f} \frac{1}{\sqrt{2}} \sum_k (-1)^{f(k)} |k\rangle \\ &\xrightarrow{H} \frac{1}{2} \sum_x \sum_k (-1)^{f(k)+(kx)} |x\rangle \end{aligned}$$

The probability *amplitude* of measuring $|0\rangle$ is:

$$A_0 = \langle 0| \frac{1}{2} \sum_x \sum_k (-1)^{f(k)+kx} |x\rangle = \frac{1}{2} \sum_k (-1)^{f(k)} = \begin{cases} \pm 1 & f \text{ is constant} \\ 0 & f \text{ is balanced} \end{cases}$$

Hence, the probability of measuring 0 is:

$$P_0 = |A_0|^2 = \begin{cases} 1 & f \text{ is constant} \\ 0 & f \text{ is balanced} \end{cases}$$

Hence, when the measurement result is 0, f is constant, and otherwise f is balance.

Deutsch Algorithm with Environmental Noise:

Now suppose the control qubit interact with the environment when we perform U_f such that $|k\rangle \to |k\rangle |e_k\rangle$, we then have:

$$\begin{aligned} |0\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}} \sum_k |k\rangle \\ &\xrightarrow{U_f} \frac{1}{\sqrt{2}} \sum_k (-1)^{f(k)} |k\rangle \\ &\xrightarrow{env} \frac{1}{\sqrt{2}} \sum_k (-1)^{f(k)} |k\rangle |e_k\rangle \\ &\xrightarrow{H} \frac{1}{2} \sum_x \sum_k (-1)^{f(k)+kx} |x\rangle |e_k\rangle \end{aligned}$$

Note that the state after environment interation: $\frac{1}{\sqrt{2}} \sum_k (-1)^{f(k)} |k\rangle |e_k\rangle$ is normalised. This is because even though $|e_0\rangle$ and $|e_1\rangle$ are not orthogonal to each other, the full two-qubit states $|0, e_0\rangle$ and $|1, e_1\rangle$ are orthogonal to each other.

Now the probability of measuring 0 is just the expectation value of the projection operator $|0\rangle\langle 0| \otimes I$:

$$\begin{aligned} P_0 &= \left(\frac{1}{2}\right)^2 \sum_{x,x'} \langle x'|0\rangle \langle 0|x\rangle \sum_{k,k'} \langle e_{k'}|e_k\rangle (-1)^{f(k)+f(k')+kx+k'x'} \\ &= \frac{1}{4} \sum_{k,k'} \langle e_{k'}|e_k\rangle (-1)^{f(k)+f(k')} \\ &= \frac{1}{4} \left(2 + (\langle e_0|e_1\rangle + \langle e_1|e_0\rangle) (-1)^{f(0)+f(1)}\right) \\ &= \frac{1}{2} \left(1 + (-1)^{f(0)+f(1)} \operatorname{Re}\{\langle e_0|e_1\rangle\}\right) \\ &= \begin{cases} \frac{1+\operatorname{Re}\{\langle e_0|e_1\rangle\}}{2} = \frac{1+v}{2} & f \text{ is constant} \\ \frac{1-\operatorname{Re}\{\langle e_0|e_1\rangle\}}{2} = \frac{1-v}{2} & f \text{ is balanced} \end{cases} \end{aligned}$$

Following our original strategy of guessing f is constant upon measuring 0, there is now a $\frac{1-v}{2}$ probability that f is actually balanced and we got it wrong.

There are two extremes to look at:

- $v = 1$: We have the perfect noiseless outcome again.

  $v = 1$ means that $|e_0\rangle = |e_1\rangle = |e\rangle$. Hence, after interaction with the environment, the resultant state is $\left(\frac{1}{\sqrt{2}} \sum_k (-1)^{f(k)} |k\rangle\right) |e\rangle$ which is just the noiseless system tensor with the environment state $|e\rangle$. In this case the environment is not entangled with our system and will not affect our results at all.

- $v = 0$: We have a completely random outcome.

  $v = 0$ means that $|e_0\rangle$ is orthogonal to $|e_1\rangle$. Hence, after interaction with the environment, the resultant state $\frac{1}{\sqrt{2}} \sum_k (-1)^{f(k)} |k, e_k\rangle$ has maximum entanglement between the system and the environment, it is essentially a bell state $\frac{1}{\sqrt{2}} \sum_k (-1)^{f(k)} |k, k\rangle$. We know that if we measure out one of the qubit in a bell state and discard the measurement result, the remaining qubit will become maximally mixed since the two qubits are completely correlated. Similarly, in this case since we do not have access to the environment qubit, our system will have completely random outcome.