1. (a) (10 points) Is it possible to output $n+1$ copies of an unknown qubit $|\varphi\rangle$ given n copies of $|\varphi\rangle$ together with $|0\rangle$ for some n? That is, is it possible to quantumly implement the map

$$|\varphi\rangle^{\otimes n} \otimes |0\rangle \mapsto |\varphi\rangle^{\otimes(n+1)}$$

for some n, or is it impossible for all n?

Solution: Suppose a unitary map U exists such that

$$U : |\varphi\rangle^{\otimes n} \otimes |0\rangle \mapsto |\varphi\rangle^{\otimes(n+1)}.$$

Note that as U is unitary, $UU^\dagger = U^\dagger U = I$. Let $|\varphi\rangle = \begin{pmatrix}\alpha_\varphi \\ \beta_\varphi\end{pmatrix}$ and $|\psi\rangle = \begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}$ be arbitrary two qubits. Then

$$\begin{aligned}
\langle\varphi|\psi\rangle^n &= \left(\begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}\right)^n \\
&= \begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}^{\otimes n}\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes n} \\
&= \left(\begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}^{\otimes n}\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes n}\right)\langle 0|0\rangle \\
&= \left(\begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}^{\otimes n}\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes n}\right)\left(\begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}1 \\ 0\end{pmatrix}\right) \\
&= \left(\begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}^{\otimes n} \otimes \begin{pmatrix}1 & 0\end{pmatrix}\right)\left(\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes n} \otimes \begin{pmatrix}1 \\ 0\end{pmatrix}\right) \\
&= \left(\begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}^{\otimes n} \otimes \begin{pmatrix}1 & 0\end{pmatrix}\right)U^\dagger U\left(\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes n} \otimes \begin{pmatrix}1 \\ 0\end{pmatrix}\right) \\
&= \left(U\left(\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes n} \otimes \begin{pmatrix}1 \\ 0\end{pmatrix}\right)\right)^\dagger U\left(\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes n} \otimes \begin{pmatrix}1 \\ 0\end{pmatrix}\right) \\
&= \left(\begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}^{\otimes n} \otimes \begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}\right)\left(\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes n} \otimes \begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}\right) \\
&= \begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}^{\otimes(n+1)}\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes(n+1)} \\
&= \left(\begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}\right)^{n+1} \\
&= \langle\varphi|\psi\rangle^{n+1}.
\end{aligned}$$

That is, $\langle\varphi|\psi\rangle^n(\langle\varphi|\psi\rangle - 1) = 0$. Thus $\langle\varphi|\psi\rangle \in \{0, 1\}$, which does not necessarily hold for arbitrary qubits. □

(b) (10 points) Can you generalize/strengthen your result?

Solution: We strengthen this assertion to the following.
There is does not exist a unitary map

$$U : |\varphi\rangle^{\otimes n} \otimes |\rho\rangle^{\otimes m} \mapsto |\varphi\rangle^{\otimes n+m}$$

for every qubit $|\varphi\rangle$, where $|\rho\rangle = \alpha_\rho |0\rangle + \beta_\rho |1\rangle$ is some fixed qubit and $n, m \in \mathbb{N}$.

The proof follows a similar lines to the proof of the original assertion. Let $|\varphi\rangle = \begin{pmatrix}\alpha_\varphi \\ \beta_\varphi\end{pmatrix}$ and

$|\psi\rangle = \begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}$ be arbitrary two qubits. Then

$$\begin{aligned}
\langle\varphi|\psi\rangle^n &= \left(\begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}\right)^n \\
&= \begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}^{\otimes n}\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes n} \\
&= \left(\begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}^{\otimes n}\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes n}\right)\langle\rho|\rho\rangle^m \\
&= \left(\begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}^{\otimes n}\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes n}\right)\left(\begin{pmatrix}\overline{\alpha}_\rho & \overline{\beta}_\rho\end{pmatrix}\begin{pmatrix}\alpha_\rho \\ \beta_\rho\end{pmatrix}\right)^m \\
&= \left(\begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}^{\otimes n}\otimes\begin{pmatrix}\overline{\alpha}_\rho & \overline{\beta}_\rho\end{pmatrix}^{\otimes m}\right)\left(\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes n}\otimes\begin{pmatrix}\alpha_\rho \\ \beta_\rho\end{pmatrix}^{\otimes m}\right) \\
&= \left(\begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}^{\otimes n}\otimes\begin{pmatrix}\overline{\alpha}_\rho & \overline{\beta}_\rho\end{pmatrix}^{\otimes m}\right)U^\dagger U\left(\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes n}\otimes\begin{pmatrix}\alpha_\rho \\ \beta_\rho\end{pmatrix}^{\otimes m}\right) \\
&= \left(U\left(\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes n}\otimes\begin{pmatrix}\alpha_\rho \\ \beta_\rho\end{pmatrix}^{\otimes m}\right)\right)^\dagger U\left(\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes n}\otimes\begin{pmatrix}\alpha_\rho \\ \beta_\rho\end{pmatrix}^{\otimes m}\right) \\
&= \left(\begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}^{\otimes n}\otimes\begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}^{\otimes m}\right)\left(\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes n}\otimes\begin{pmatrix}\alpha_\rho \\ \beta_\rho\end{pmatrix}^{\otimes m}\right) \\
&= \begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}^{\otimes(n+m)}\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}^{\otimes(n+m)} \\
&= \left(\begin{pmatrix}\overline{\alpha}_\varphi & \overline{\beta}_\varphi\end{pmatrix}\begin{pmatrix}\alpha_\psi \\ \beta_\psi\end{pmatrix}\right)^{n+m} \\
&= \langle\varphi|\psi\rangle^{n+m}.
\end{aligned}$$

Thus $\langle\varphi|\psi\rangle^n(\langle\varphi|\psi\rangle^m - 1) = 0$. Thus $\langle\varphi|\psi\rangle$ is either 0 or an mth root of unity, neither of which is necessarily true for arbitrary qubits. $\square$

2. A challenger holds two qubits $|0\rangle$ and $\alpha|0\rangle + \beta|1\rangle$, where $|\beta|$ should be thought as small so that the two qubits are "close". It picks random bit $c \in \{0,1\}$, and hands out the first qubit to a distinguisher if $c = 0$, and the second qubit if $c = 1$. The advantage of the distinguisher is defined as its probability of correctly guessing c minus $1/2$ (i.e., how much better than "trivial guessing" it does).

   (a) (5 points) Show there is a distinguisher that can win this game with advantage $\Omega(|\beta|^2)$ by measurement in the standard basis.

Solution: We propose the following strategy. Measure the qubit in the standard basis $(|0\rangle, |1\rangle)$.

1. If $|0\rangle$ is measured, guess $c = 0$.
2. If $|1\rangle$ is measured, guess $c = 1$.

We now prove this has advantage $\Omega(|\beta|^2)$.
Let $|m\rangle$ be the qubit given to the distinguisher. If $|m\rangle = |0\rangle$, then they measure $|0\rangle$ with probability 1 and $|1\rangle$ with probability 0. If $|m\rangle = \alpha|0\rangle + \beta|1\rangle$, then they measure $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$. Then

$$\begin{aligned} P(\text{correct}) &= P(\text{correct} \mid |m\rangle = |0\rangle)P(|m\rangle = |0\rangle) \\ &\quad + P(\text{correct} \mid |m\rangle = \alpha|0\rangle + \beta|1\rangle)P(|m\rangle = \alpha|0\rangle + \beta|1\rangle) \\ &= \frac{1}{2}P(\text{correct} \mid |m\rangle = |0\rangle) + \frac{1}{2}P(\text{correct} \mid |m\rangle = \alpha|0\rangle + \beta|1\rangle) \\ &= \frac{1}{2}(1) + \frac{1}{2}(|\beta|^2) \\ &= \frac{1}{2} + \frac{1}{2}|\beta|^2. \end{aligned}$$

Thus the advantage is $\frac{1}{2}|\beta|^2 = \Omega(|\beta|^2)$.

   (b) (10 points) Show it is possible to distinguish with advantage $\Omega(|\beta|)$, for instance by either applying a unitary transformation before measurement, or by measuring in a different basis.

Solution: We parameterise α and β as positive real numbers with $n \in \mathbb{N}$; that is, $\alpha, \beta : \mathbb{N} \to \mathbb{C}$ such that $\alpha(n) \to 1$ and $\beta(n) \to 0$ as $n \to \infty$. Note, we must have $|\alpha(n)|^2 + |\beta(n)|^2 = 1$.
We recall that $f(n) = \Omega(g(n))$ if and only if

$$\liminf_{n\to\infty} \frac{|f(n)|}{g(n)} > 0,$$

with the assumption that $g(n) > 0$ for sufficiently large n.
Let $|\varphi\rangle = \alpha(n)|0\rangle + \beta(n)|1\rangle$, and pick the measurement basis $(|+\rangle, |-\rangle)$.
Note that the angle between $|0\rangle$ and $|+\rangle$ is $\pi/4$, thus measuring $|0\rangle$ yields $|+\rangle$ with probability $\cos^2 \pi/4 = 1/2$, and $|-\rangle$ with probability also $1/2$.
Measuring $|\varphi\rangle$ gives $|+\rangle$ with probability

$$\begin{aligned} |\langle\varphi|+\rangle|^2 &= \left| \begin{pmatrix} \overline{\alpha}(n) & \overline{\beta}(n) \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} \right|^2 \\ &= \left| \frac{1}{\sqrt{2}}(\overline{\alpha}(n) + \overline{\beta}(n)) \right|^2 \\ &= \frac{1}{2}|\alpha(n) + \beta(n)|^2 \\ &= \frac{1}{2}(\alpha(n)\overline{\alpha}(n) + \beta(n)\overline{\beta}(n) + \overline{\alpha}(n)\beta(n) + \alpha(n)\overline{\beta}(n)) \\ &= \frac{1}{2}(1 + \overline{\alpha}(n)\beta(n) + \alpha(n)\overline{\beta}(n)). \end{aligned}$$

As the sum of measuring $|+\rangle$ and $|-\rangle$ must sum to 1, measuring $|\varphi\rangle$ gives $|-\rangle$ with probability

$$\frac{1}{2}(1 - \overline{\alpha}(n)\beta(n) - \alpha(n)\overline{\beta}(n)).$$

We now outline our strategy.

(I) If $\overline{\alpha}(n)\beta(n) + \alpha(n)\overline{\beta}(n) > 0$, then we guess $c = 0$ if we measure $|-\rangle$ and $c = 1$ if we measure $|+\rangle$.

(II) If $\overline{\alpha}(n)\beta(n) + \alpha(n)\overline{\beta}(n) < 0$, then we guess $c = 0$ if we measure $|+\rangle$ and $c = 1$ if we measure $|-\rangle$.

Note that if $\overline{\alpha}(n)\beta(n) + \alpha(n)\overline{\beta}(n) = 0$, then $\beta(n) = 0$ and $\alpha(n) = 1$, which we disregard (we assume $|\beta(n)|$ is *close* to 0, but not quite 0).
We consider the advantage of strategy (I) first. The probability of success is

$$\begin{aligned} p_{\mathrm{I}}(n) &= \frac{1}{2}\left(\frac{1}{2}\right) + \frac{1}{2}\left(\frac{1}{2}(1 + \overline{\alpha}(n)\beta(n) + \alpha(n)\overline{\beta}(n))\right) \\ &= \frac{1}{2} + \frac{1}{2}(\overline{\alpha}(n)\beta(n) + \alpha(n)\overline{\beta}(n)). \end{aligned}$$

Thus the advantage is

$$a_{\mathrm{I}}(n) = \frac{1}{2}(\overline{\alpha}(n)\beta(n) + \alpha(n)\overline{\beta}(n)).$$

Similarly, for strategy (II),

$$\begin{aligned} p_{\mathrm{II}}(n) &= \frac{1}{2}\left(\frac{1}{2}\right) + \frac{1}{2}\left(\frac{1}{2}(1 - \overline{\alpha}(n)\beta(n) - \alpha(n)\overline{\beta}(n))\right) \\ &= \frac{1}{2} - \frac{1}{2}(\overline{\alpha}(n)\beta(n) + \alpha(n)\overline{\beta}(n)). \end{aligned}$$

So the advantage is

$$a_{\mathrm{II}}(n) = -\frac{1}{2}(\overline{\alpha}(n)\beta(n) + \alpha(n)\overline{\beta}(n)).$$

Thus, our overall advantage is

$$\begin{aligned} a(n) &= \begin{cases} a_{\mathrm{I}}(n) & \text{if } \overline{\alpha}(n)\beta(n) + \alpha(n)\overline{\beta}(n) > 0, \\ a_{\mathrm{II}}(n) & \text{if } \overline{\alpha}(n)\beta(n) + \alpha(n)\overline{\beta}(n) < 0. \end{cases} \\ &= \frac{1}{2}|\overline{\alpha}(n)\beta(n) + \alpha(n)\overline{\beta}(n)| \end{aligned}$$

See that

$$\liminf_{n\to\infty}\left(\frac{a(n)}{|\beta(n)|}\right) = \liminf_{n\to\infty}\left(\frac{|\overline{\alpha}(n)\beta(n) + \alpha(n)\overline{\beta}(n)|}{2|\beta(n)|}\right) > 0.$$

Thus $a(n) = \Omega(|\beta(n)|)$.

(c) (20 points) Is it possible to do even better?

Solution: The Helstrom-Holevo bound establishes an upper bound to the amount of information that can be known about a quantum state.
Theorem. If $|\varphi\rangle$ is either in state $|\varphi_a\rangle$ or $|\varphi_b\rangle$, where $|\langle\varphi_a|\varphi_b\rangle| = \cos\theta$, then an optimal strategy for correctly inferring state $|\varphi\rangle$ is less than or equal to $\frac{1}{2}(1 + \sin\theta)$. Furthermore, this bound can be achieved by choosing the measurement basis as the eigenvectors of

$$|\varphi_a\rangle\langle\varphi_a| - |\varphi_b\rangle\langle\varphi_b|.$$

Let $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$. Through careful consideration, the eigenvalues of $|0\rangle\langle 0| - |\varphi\rangle\langle\varphi|$ are $|\beta|$ and $-|\beta|$, and some corresponding eigenvectors are

$$\begin{pmatrix} \frac{\alpha\overline{\beta}}{|\beta|(|\beta|+1)} \\ 1 \end{pmatrix}, \qquad \begin{pmatrix} \frac{-|\beta|(|\beta|+1)}{\overline{\alpha}\beta} \\ 1 \end{pmatrix}$$

respectively. Our optimal measurement basis would be normalised forms of these vectors. Using this basis, our optimal strategy has probability of success is $\frac{1}{2}(1+\sin\theta)$, and so our advantage is

$$\begin{aligned} a &= \frac{1}{2}\sin\theta \\ &= \frac{1}{2}\sqrt{1-\cos^2\theta} \\ &= \frac{1}{2}\sqrt{1-|\langle 0|\varphi\rangle|^2} \\ &= \frac{1}{2}\sqrt{1-\left|\begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}\alpha \\ \beta\end{pmatrix}\right|^2} \\ &= \frac{1}{2}\sqrt{1-|\alpha|^2} \\ &= \frac{1}{2}|\beta| \\ &= \Theta(|\beta|). \end{aligned}$$

Thus we cannot perform any better than this $\Omega(\beta)$ bound.

3. (30 points) Alice and Bob share an EPR pair. Alice, in addition, holds a random bit $x \in \{0, 1\}$ that she wishes to communicate to Bob with no interaction. Prove that it is not possible to do this with the following method. First, Alice performs a measurement of her qubit in a basis with real amplitudes. Next Bob measures his qubit in a second basis with real amplitudes, and outputs a guess x' for x based on the measurement outcome. (Hint: You may use a well-known property of the EPR pair. If you do so, you should state and prove this property.)

Solution: We first have two assertion to make.

Lemma 1. Let $|u\rangle = a_u |0\rangle + b_u |1\rangle$ be a real unit vector in $\mathbb{C}^2$ with the standard inner product. Then $|u\rangle$ and a real unit vector $|v\rangle = a_v |0\rangle + b_v |1\rangle$ are orthonormal if and only if

$$a_v = \mp b_u, \qquad b_v = \pm a_u.$$

Proof. As $|u\rangle$ and $|v\rangle$ are orthogonal, we have

$$\begin{aligned} \langle u|v\rangle &= 0 \\ \begin{pmatrix} \overline{a}_u & \overline{b}_u \end{pmatrix} \begin{pmatrix} a_v \\ b_v \end{pmatrix} &= 0 \\ \overline{a}_u a_v + \overline{b}_u b_v &= 0 \\ a_u a_v + b_u b_v &= 0 \end{aligned}$$

and so $a_u a_v = -b_u b_v$. As $|u\rangle$ and $|v\rangle$ are unit vectors, we have $a_u^2 + b_u^2 = 1$ and $a_v^2 + b_v^2 = 1$. Thus

$$\begin{aligned} a_u a_v &= -b_u b_v \\ a_u^2 a_v^2 &= b_u^2 b_v^2 \\ (1 - b_u^2) a_v^2 &= b_u^2 b_v^2 \\ a_v^2 &= (a_v^2 + b_v^2) b_u^2 \\ a_v^2 &= b_u^2 \\ a_v &\in \{b_u, -b_u\} \end{aligned} \qquad \begin{aligned} a_u a_v &= -b_u b_v \\ a_u^2 a_v^2 &= b_u^2 b_v^2 \\ a_u^2 a_v^2 &= (1 - a_u^2) b_v^2 \\ a_u^2 (a_v^2 + b_v^2) &= b_v^2 \\ a_u^2 &= b_v^2 \\ b_v &\in \{a_u, -a_u\}. \end{aligned}$$

If $|v\rangle \in \{b_u |0\rangle + a_u |1\rangle, -b_u |0\rangle - a_u |1\rangle\}$, then $\langle u|v\rangle = 1$. If $|v\rangle \in \{-b_u |0\rangle + a_u |1\rangle), b_u |0\rangle - a_u |1\rangle\}$, then $\langle u|v\rangle = 0$, the required result. $\square$

Next we have an assertion on the invariance of the Bell state (or EPR pairs).

Lemma 2. Let $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ be the Bell state (sometimes denoted $|\Phi^+\rangle$). Let $(|u\rangle, |v\rangle)$ be a real orthonormal basis (in $\mathbb{C}^2$ with the standard inner product). Then

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|uu\rangle + |vv\rangle).$$

Proof. Let $|u\rangle = a|0\rangle + b|1\rangle$ for some $a, b \in \mathbb{R}$ with $a^2 + b^2 = 1$. As $|u\rangle$ and $|v\rangle$ are orthonormal, by Lemma 1, we have $|v\rangle = \mp b|0\rangle + \pm a|1\rangle$. Thus

$$\begin{aligned} \frac{1}{\sqrt{2}}(|uu\rangle + |vv\rangle) &= \frac{1}{\sqrt{2}}((|u\rangle \otimes |u\rangle) + (|v\rangle \otimes |v\rangle)) \\ &= \frac{1}{\sqrt{2}}\left((a|0\rangle + b|1\rangle) \otimes (a|0\rangle + b|1\rangle) + (\mp b|0\rangle + \pm a|1\rangle) \otimes (\mp b|0\rangle + \pm a|1\rangle)\right) \\ &= \frac{1}{\sqrt{2}}((a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|00\rangle) + (a^2|00\rangle - ab|01\rangle - ab|10\rangle + b^2|00\rangle)) \\ &= \frac{1}{\sqrt{2}}((a^2 + b^2)|00\rangle + (a^2 + b^2)|11\rangle) \\ &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \end{aligned}$$

$\square$

We now answer the question. Suppose Alice measures in real basis $(|u_A\rangle, |v_A\rangle)$ and Bob measures in real basis $(|u_B\rangle, |v_B\rangle)$. We note that measurement bases must be orthonormal, to avoid ambiguity. Let θ be the angle between $|u_A\rangle$ and $|u_B\rangle$. Suppose that Bob has some strategy of correctly guessing x based on his measurement; that is, a function $f : \{|u_B\rangle, |v_B\rangle\} \to \{0, 1\}$ such that f applied to Bob's measurement gives x.

First, Alice measures her qubit. By Lemma 2,

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|u_A u_A\rangle + |v_A v_A\rangle)$$

and thus Alice measures $|u_A\rangle$ with probability 1/2, and $|v_A\rangle$ with probability 1/2, irrespective of the value of x.

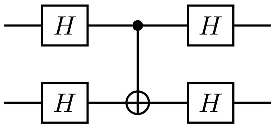
Consider the scenario in which Alice measures $|u_A\rangle$. Then Bob will measure $|u_B\rangle$ with probability $\cos^2\theta$, and $|v_B\rangle$ with probability $\sin^2\theta$, again irrespective of the value of x.

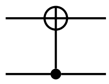
If $\cos^2\theta \neq 0$, then Bob will measure $|u_B\rangle$ with a non-zero probability. In such a scenario, if $x = 0$, then $f(|u_B\rangle) = 0$. But if $x = 1$, then $f(|u_B\rangle) = 1$; a contradiction.

If $\cos^2\theta = 0$, then Bob will measure $|v_B\rangle$ with probability 1. In this scenario, if $x = 0$, then $f(|v_B\rangle) = 0$. But if $x = 1$, then $f(|v_B\rangle) = 1$; a contradiction. $\square$

A similar result holds even if Alice chooses a basis based on the value of x, given the invariance of the Bell state. Regardless of the basis chosen, Alice will measure either basis element with probability 1/2.

4. (15 points) Show that the following two circuits are functionally equivalent.





Solution: An equivalent statement of this question is

$$\text{CNOT} = (H \otimes H)\ \overline{\text{CNOT}}\ (H \otimes H).$$

We first look at some truth tables for CNOT gates. Note $\overline{\text{CNOT}}$ is the CNOT gate with the input source and target qubits swapped.

Input		CNOT		$\overline{\text{CNOT}}$	
A	B	A	B	A	B
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$

Pick the basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Then we have the matrices

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad \overline{\text{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

For H, we have

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Thus

$$H \otimes H = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

We then conclude,

$$\begin{aligned}
(H \otimes H)\ \overline{\text{CNOT}}\ (H \otimes H) &= \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \\
&= \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\
&= \text{CNOT}.
\end{aligned}$$