CS 498 QC Fall 2023 Wenqi He (wenqihe2)

Homework 6 Problem 1

a

The largest value k can take is $\lfloor m/2 \rfloor = (m-1)/2$.

Proof: We could construct a bit-flip decoder that computes the majority of m qubits and applies X to every qubit that is different from the majority. We could then construct a phase-flip decoder that first applies $H^{\otimes m}$, then applies the bit-flip decoder. As with the original 9-qubit code, we first apply bit-flip decoding to each bit-flip code of size m, and then apply phase-flip decoding to the resulting m qubits.

The error unitary E that applies to the k qubits can be written as

$$\begin{aligned} E &= U_1 \otimes U_2 \otimes \cdots \otimes U_k \\ &= \left(\sum_{U \in \{I,X,Z,XZ\}} a_1^{(U)} U \right) \otimes \left(\sum_{U \in \{I,X,Z,XZ\}} a_2^{(U)} U \right) \otimes \cdots \otimes \left(\sum_{U \in \{I,X,Z,XZ\}} a_k^{(U)} U \right) \\ &= \sum_{U \in \{I,X,Z,XZ\}^{\otimes k}} b^{(U)} U \end{aligned}$$

where the basis is a set of 4^k matrices.

$$\{I,X,Z,XZ\}^{\otimes k} := \{U_1 \otimes U_2 \otimes \cdots \otimes U_k \mid \forall 1 \le i \le k, U_i \in \{I,X,Z,XZ\}\}$$

When $k \le \lfloor m/2 \rfloor$, for each $U \in \{I,X,Z,XZ\}^{\otimes k}$, there are at most $\lfloor m/2 \rfloor$ bit flips in each bit-flip code, which can be corrected. After bit-flip decoding, there are at most $\lfloor m/2 \rfloor$ phase flips in the resulting phase-flip code, which can also be corrected. By linearity, any arbitrary error E can be corrected:

$$C(E\left|\phi\right\rangle\left|0^n\right\rangle) = \sum_{U \in \{I,X,Z,XZ\}^{\otimes k}} b^{(U)} C(U\left|\phi\right\rangle\left|0^n\right\rangle) = \sum_{U \in \{I,X,Z,XZ\}^{\otimes k}} b^{(U)} \left|\phi\right\rangle\left|g_U\right\rangle = \left|\phi\right\rangle\left|g\right\rangle.$$

When $k > \lfloor m/2 \rfloor$, the decoding circuit can produce incorrect results. For example, suppose there are $k = \lfloor m/2 \rfloor + 1 = (m+1)/2$ phase flips at position $m, 2m, \cdots, km$. After bit-flip decoding, the majority of the m qubits still have phase flip errors, so phase-flip decoding will give the wrong result. □

b

The probability is 0.

Proof: Each bit-flip code of size m always decodes to $\left|+\right\rangle$, regardless of how many qubits are flipped – even if the majority of the m qubits are flipped, it still decodes to $\left|+\right\rangle$, because both amplitudes are equal. Therefore, the bit-flip decoding output is always $\left|+^m\right\rangle$, which then decodes to $\left|0\right\rangle$ after phase-flip decoding. □

CS 498 QC Fall 2023 Wenqi He (wenqihe2)

Homework 6 Problem 2

a

If it's possible to perform tomography on a single copy of an arbitrary pure state, then we already have all the information we need to prepare the state — i.e., cloning is possible.

Eve can figure out $\{\theta_i\}$ and $\{x_i\}$ by herself without the $\{\theta_i\}$ message from Alice. Using $\{\theta_i\}$ and $\{x_i\}$, Eve can reconstruct $\left\{|x_i\rangle_{\theta_i}\right\}$, flip $|x_1\rangle_{\theta_1}$ (turn it into $|\neg x_1\rangle_{\theta_1}$), and send these qubits to Bob. Alice picks a subset S that doesn't contain 1 with probability

$$\binom{N-1}{|S|}\Big/\binom{N}{|S|} = 1 - \frac{|S|}{N},$$

where N is the number of samples. If S doesn't contain 1, Bob's check passes, and Eve establishes $k_1 = x_1 \cdots$ with Alice and $k_2 = \neg x_1 \cdots \neq k_1$ with Bob.

b

If the classical channel is not authenticated, Eve can first perform QKD with Alice to establish k_1, pretending to be Bob. Then she can perform QKD with Bob to establish k_2, pretending to be Alice. By playing the role of Alice, Eve has the freedom to choose any $k_2 \neq k_1$.

CS 498 QC Fall 2023 Wenqi He (wenqihe2)

Homework 5 Problem 1

a

First apply $U_f = U_T \cdots U_2 U_1$ to the first n and the last m qubits. The state becomes

$$|x\rangle\, |y\rangle\, |f(x)\rangle\, |g(x)\rangle$$

Then apply CNOT, using $|f(x)\rangle$ as control and $|y\rangle$ as target. The state becomes

$$|x\rangle\, |y \oplus f(x)\rangle\, |f(x)\rangle\, |g(x)\rangle$$

Finally, apply $U_f^{-1} = U_1^{-1} U_2^{-1} \cdots U_T^{-1}$ to the first n and last m qubits. The state becomes

$$|x\rangle\, |y \oplus f(x)\rangle\, |0^m\rangle$$

b

1. Apply H to the $(n+1)$-th qubit.
2. Apply $\hat{O}_f$ to the first $n+1$ qubits.
3. Apply H again to the $(n+1)$-th qubit.

Proof: After step 1, the state is

$$|x\rangle \left(\frac{1}{\sqrt{2}} |0\rangle + \frac{(-1)^y}{\sqrt{2}} |1\rangle \right) |0^m\rangle$$

After step 2, the state is

$$\begin{aligned} &|x\rangle \left((-1)^{0 \cdot f(x)} \frac{1}{\sqrt{2}} |0\rangle + (-1)^{1 \cdot f(x)} \frac{(-1)^y}{\sqrt{2}} |1\rangle \right) |0^m\rangle \\ &= |x\rangle \left(\frac{1}{\sqrt{2}} |0\rangle + \frac{(-1)^{y+f(x)}}{\sqrt{2}} |1\rangle \right) |0^m\rangle = |x\rangle \left(\frac{1}{\sqrt{2}} |0\rangle + \frac{(-1)^{y \oplus f(x)}}{\sqrt{2}} |1\rangle \right) |0^m\rangle \end{aligned}$$

After step 3, the state is

$$|x\rangle\, |y \oplus f(x)\rangle\, |0^m\rangle$$

□

CS 498 QC Fall 2023 Wenqi He (wenqihe2)

Homework 5 Problem 2

a

$$
\begin{aligned}
|\psi\rangle &= \frac{1}{\sqrt{2^n}} \sum_s |s\rangle \\
|\psi\rangle \langle\psi| \sum_x \alpha_x |x\rangle = |\psi\rangle \sum_x \alpha_x \langle \psi \,|\, x\rangle &= \left(\sum_x \alpha_x \langle \psi \,|\, x\rangle \right) |\psi\rangle \\
&= \left(\sum_x \frac{\alpha_x}{\sqrt{2^n}} \right) \frac{1}{\sqrt{2^n}} \sum_s |s\rangle \\
&= \left(\sum_x \frac{\alpha_x}{2^n} \right) \sum_s |s\rangle \\
&= \mu \sum_s |s\rangle \\
(2 |\psi\rangle \langle\psi| - \mathbb{I}) \sum_x \alpha_x |x\rangle &= 2 \left(|\psi\rangle \langle\psi| \sum_x \alpha_x |x\rangle \right) - \sum_x \alpha_x |x\rangle \\
&= 2\mu \sum_x |x\rangle - \sum_x \alpha_x |x\rangle \\
&= \sum_x (2\mu - \alpha_x) |x\rangle
\end{aligned}
$$

b

We can first implement $2 |1^n\rangle \langle 1^n| - \mathbb{I}$, then $2 |0^n\rangle \langle 0^n| - \mathbb{I}$, and finally $2 |\psi\rangle \langle\psi| - \mathbb{I}$.

To implement $2 |1^n\rangle \langle 1^n| - \mathbb{I}$, we can add n ancillas $a_0, a_1, ...a_{n-1}$. First, apply the gates

$$
\begin{aligned}
A_0 &= H_{a_0} X_{a_0} \\
A_1 &= \text{CSWAP}_{x_0, x_1, a_1} \\
A_2 &= \text{CSWAP}_{a_1, x_2, a_2} \\
&\cdots \\
A_{n-1} &= \text{CSWAP}_{a_{n-2}, x_{n-1}, a_{n-1}} \\
A_n &= X_{a_n - 1}
\end{aligned}
$$

After applying these gates, $|a_0\rangle = |-\rangle$, $a_{n-1} = \neg(x_0 \wedge x_1 \wedge \cdots \wedge x_{n-1})$. Then, apply CNOT with a_{n-1} as control and a_0 as target. For basis vector $|1^n\rangle$, the control qubit is 0, so $|a_0\rangle$ is unchanged. For all other basis vectors, the control qubit is 1, so $|a_0\rangle$ becomes $-|-\rangle$ and therefore the joint state of the entire system picks up a negative sign. Finally, we apply $A_n, \cdots, A_1, A_0$ to uncompute, after which all ancillas revert to 0, and all basis vectors except $|1^n\rangle$ pick up a negative sign. In short, we can implement

$$
Z_1 = 2 |1^n\rangle \langle 1^n| - \mathbb{I}
$$

as

$$A_0 A_1 \cdots A_n \, \mathrm{CNOT}_{a_{n-1},a_0} \, A_n \cdots A_1 A_0$$

With Z_1, we can implement

$$Z_0 = X^{\otimes n} Z_1 X^{\otimes n} = 2\left(X^{\otimes n}\left|1^n\right\rangle\right)\left(\left\langle 1^n\right| X^{\otimes n}\right) - \mathbb{I} = 2\left|0^n\right\rangle\left\langle 0^n\right| - \mathbb{I}$$

Similarly, with Z_0, we can implement

$$\mathcal{D} = H^{\otimes n} Z_0 H^{\otimes n} = 2\left(H^{\otimes n}\left|0^n\right\rangle\right)\left(\left\langle 0^n\right| H^{\otimes n}\right) - \mathbb{I} = 2\left|\psi\right\rangle\left\langle\psi\right| - \mathbb{I}$$

c

Let $N = 2^n$. The initial state is

$$\left|\psi_0\right\rangle = \frac{1}{\sqrt{N}} \sum_x \left|x\right\rangle$$

The first step:

$$O_f\left|\psi_0\right\rangle = \frac{1}{\sqrt{N}} \sum_x (-1)^{f(x)}\left|x\right\rangle = \frac{1}{\sqrt{N}}\left[\left(\sum_{x \neq a_1, x \neq a_2}\left|x\right\rangle\right) - \left(\left|a_1\right\rangle + \left|a_2\right\rangle\right)\right]$$

$$\mu = \frac{1}{\sqrt{N}} \frac{(N-2) \cdot 1 + 2 \cdot (-1)}{N} = \frac{1}{\sqrt{N}} \frac{N-4}{N}$$

$$\begin{aligned}
\left|\psi_1\right\rangle &= \mathcal{D} O_f \left|\psi_0\right\rangle \\
&= \frac{1}{\sqrt{N}}\left[\left(2 \cdot \frac{N-4}{N} - 1\right)\left(\sum_{x \neq a_1, x \neq a_2}\left|x\right\rangle\right) + \left(2 \cdot \frac{N-4}{N} + 1\right)\left(\left|a_1\right\rangle + \left|a_2\right\rangle\right)\right] \\
&= \frac{1}{\sqrt{N}}\left[\left(\frac{N-8}{N}\right)\left(\sum_{x \neq a_1, x \neq a_2}\left|x\right\rangle\right) + \left(\frac{3N-8}{N}\right)\left(\left|a_1\right\rangle + \left|a_2\right\rangle\right)\right]
\end{aligned}$$

The second step:

$$O_f\left|\psi_1\right\rangle = \frac{1}{\sqrt{N}}\left[\left(\frac{N-8}{N}\right)\left(\sum_{x \neq a_1, x \neq a_2}\left|x\right\rangle\right) + \left(\frac{8-3N}{N}\right)\left(\left|a_1\right\rangle + \left|a_2\right\rangle\right)\right]$$

$$\begin{aligned}
\mu &= \frac{1}{\sqrt{N}} \frac{(N-2)\frac{N-8}{N} + 2 \cdot \frac{8-3N}{N}}{N} = \frac{1}{\sqrt{N}} \frac{(N-2)(N-8) + 2 \cdot (8-3N)}{N^2} \\
&= \frac{1}{\sqrt{N}} \frac{N^2 - 16N + 32}{N^2}
\end{aligned}$$

$$\begin{aligned}
|\psi_2\rangle &= \mathcal{D}O_f\,|\psi_1\rangle \\
&= \frac{1}{\sqrt{N}}\Bigg[\left(2\cdot\frac{N^2-16N+32}{N^2}-\frac{N-8}{N}\right)\left(\sum_{x\neq a_1,x\neq a_2}|x\rangle\right) \\
&\qquad + \left(2\cdot\frac{N^2-16N+32}{N^2}-\frac{8-3N}{N}\right)(|a_1\rangle+|a_2\rangle)\Bigg] \\
&= \frac{1}{\sqrt{N}}\left[\frac{N^2-24N+64}{N^2}\left(\sum_{x\neq a_1,x\neq a_2}|x\rangle\right)+\frac{5N^2-40N+64}{N^2}(|a_1\rangle+|a_2\rangle)\right]
\end{aligned}$$

d

Applying O_f doesn't change the state because the phase change is always $(-1)^{f(x)} = 1$. And since all amplitudes remain equal, inversion about the mean doesn't change the state either. Therefore, the state remains a uniform superposition

$$|\psi\rangle = \frac{1}{\sqrt{N}}\sum_x |x\rangle$$

no matter how many Grover steps we apply.

CS 498 QC Fall 2023 Wenqi He (wenqihe2)
Homework 4 Problem 1

a

$2^{n-1}+1$ queries.

b

Query f using 8 inputs sampled from a uniform distribution, and decide f is constant if all output are the same and balanced otherwise. This algorithm only gives a wrong answer when f is balanced but the query outputs are either all ones or all zeros, in which case

$$Pr(correct \mid balanced) = 1 - Pr(incorrect \mid balanced) = 1 - 2 \cdot 0.5^8 = 0.9921875.$$

c

We can use one ancilla qubit. First apply a H gate and a Z gate to the ancilla, resulting in

$$|x\rangle\,|-\rangle = \frac{1}{\sqrt{2}}\,|x\rangle\,|0\rangle - \frac{1}{\sqrt{2}}\,|x\rangle\,|1\rangle$$

then apply U_f, which gives us

$$|\psi\rangle = \frac{1}{\sqrt{2}}\,|x\rangle\,|0 \oplus f(x)\rangle - \frac{1}{\sqrt{2}}\,|x\rangle\,|1 \oplus f(x)\rangle = (-1)^{f(x)}\,|x\rangle\,|-\rangle$$

This circuit implements O_f if we ignore the ancilla.

d

If we measure 0^n, f must be constant, otherwise it must be balanced.

Proof:

After applying $H^{\otimes n}$, the state is

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle\,.$$

After applying O_f, the state is

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)}\,|x\rangle\,.$$

After applying the second $H^{\otimes n}$, the state is

$$\begin{aligned}
&\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \left(\frac{1}{\sqrt{2^n}} \sum_{s\in\{0,1\}^n} (-1)^{x\cdot s} |s\rangle \right) \\
&= \frac{1}{2^n} \sum_{s\in\{0,1\}^n} \left(\sum_{x\in\{0,1\}^n} (-1)^{f(x)+x\cdot s} \right) |s\rangle
\end{aligned}$$

If $f(x) = c$ is constant, then the sum in parentheses is

$$\sum_{x\in\{0,1\}^n} (-1)^{c+x\cdot s} = (-1)^c \sum_{x\in\{0,1\}^n} (-1)^{x\cdot s}$$

For any $s \neq 0^n$, let i be any index such that $s_i = 1$, then,

$$\begin{aligned}
\sum_{x\in\{0,1\}^n} (-1)^{x\cdot s} &= \sum_{x\in\{0,1\}^n, x_i=0} (-1)^{x\cdot s} + \sum_{x\in\{0,1\}^n, x_i=1} (-1)^{x\cdot s} \\
&= \sum_{x\in\{0,1\}^n, x_i=0} (-1)^{x\cdot s} + \sum_{x\in\{0,1\}^n, x_i=0} (-1)^{x\cdot s+1} \\
&= \sum_{x\in\{0,1\}^n, x_i=0} (-1)^{x\cdot s} - \sum_{x\in\{0,1\}^n, x_i=0} (-1)^{x\cdot s} = 0
\end{aligned}$$

Therefore, the state is

$$\frac{(-1)^c}{2^n} \cdot 2^n |0^n\rangle = (-1)^c |0^n\rangle,$$

and we always measure 0^n. However, if f is balanced, then

$$\begin{aligned}
\sum_{x\in\{0,1\}^n} (-1)^{f(x)+x\cdot s} &= \sum_{x\in\{0,1\}^n, f(x)=0} (-1)^{f(x)+x\cdot s} + \sum_{x\in\{0,1\}^n, f(x)=1} (-1)^{f(x)+x\cdot s} \\
&= \sum_{x\in\{0,1\}^n, f(x)=0} (-1)^{x\cdot s} - \sum_{x\in\{0,1\}^n, f(x)=1} (-1)^{x\cdot s}.
\end{aligned}$$

For $s = 0^n$, the sum evaluates to

$$2^{n-1} - 2^{n-1} = 0,$$

so the probability of measuring 0^n is 0.

CS 498 QC Fall 2023 Wenqi He (wenqihe2)

Homework 4 Problem 2

a

Let $|\psi\rangle$ be the unit eigenvector associated with λ, then

$$\|U|\psi\rangle\| = \|\lambda|\psi\rangle\| = |\lambda| \cdot \||\psi\rangle\| = |\lambda| = 1,$$

so $\lambda = e^{2\pi i\phi}$ for some ϕ.

b

Since U is unitary, it preserves the norm, then for any vector $|\psi\rangle$

$$\left\|U^j|\psi\rangle\right\| = \left\|U^{j-1}|\psi\rangle\right\| = \cdots = \|\psi\|,$$

U^j also preserves the norm, therefore U^j is also unitary.

c

For convenience, we'll use little-endian order for the qubits in $|j\rangle$. We can implement the unitary by applying a cU^{2^k} gate for each $k \in \{0, 1, \cdots, n-1\}$, using the k-th qubit as the control qubit. The output state is

$$|j\rangle \prod_{k=0}^{n-1} \left(U^{2^k}\right)^{j_k} |b\rangle = |j\rangle U^{\sum\limits_{k=0}^{n-1} j_k 2^k} |b\rangle = |j\rangle U^j |b\rangle$$

d

After applying the $H^{\otimes n}$ gate, the state is

$$|+\rangle^{\otimes n} |\psi\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle |\psi\rangle$$

After applying the unitary in (c), the final state is

$$\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle U^j |\psi\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j\phi} |j\rangle |\psi\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_N^{jN\phi} |j\rangle |\psi\rangle$$

e

We can discard $|\psi\rangle$ and apply (inverse) QFT_N to the first n qubits. The final state is

$$\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\omega_N^{jN\phi}\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\omega_N^{-jk}|k\rangle = \frac{1}{N}\sum_{k=0}^{N-1}\sum_{j=0}^{N-1}\omega_N^{j(N\phi-k)}|k\rangle$$

Note that

$$N\phi = 2^n\sum_{j=1}^{n}\phi_j 2^{-j} = \sum_{j=1}^{n}\phi_j 2^{n-j}$$

is a n-bit integer. Now, if $(N\phi - k) \not\equiv 0 \pmod{N}$,

$$\sum_{j=0}^{N-1}\omega_N^{j(N\phi-k)} = \frac{1}{\omega_N^{N\phi-k}-1}\left(\omega_N^{N(N\phi-k)}-1\right) = 0$$

If $(N\phi - k) \equiv 0 \pmod{N}$,

$$\sum_{j=0}^{N-1}\omega_N^{j(N\phi-k)} = \sum_{j=0}^{N-1}1 = N,$$

And since $0 \le N\phi < N$ and $0 \le k < N$, we know that $-N < N\phi - k < N$, so $(N\phi - k) \equiv 0 \pmod{N}$ if and only if $N\phi = k$. Therefore, only one term remains, and the final state is exactly

$$|N\phi\rangle.$$

If Bob measures the first n qubits, with probability 1 he obtains $N\phi$, which encodes the secret. However, the secret should be decoded in the reverse order, i.e. the j-th secret is represented by the $(n-j)$-th qubit.

CS 498 QC Fall 2023 Wenqi He (wenqihe2)
Homework 4 Problem 3

a

$$f(0) = 3^0 \bmod 20 = 1, \quad f(1) = 3^1 \bmod 20 = 3, \quad f(2) = 3^2 \bmod 20 = 9$$
$$f(3) = 3^3 \bmod 20 = 7, \quad f(4) = 3^4 \bmod 20 = 1 = f(0)$$

Therefore, $p = 4$.

b

Since $\left(a^{p/2} - 1\right)\left(a^{p/2} + 1\right) = a^p - 1 = kN$, then unless N divides either $a^{p/2} - 1$ or $a^{p/2} + 1$, $\gcd\left(a^{p/2} - 1, N\right)$ and $\gcd\left(a^{p/2} + 1, N\right)$ must be non-trivial factors of N, because if, for example, $\gcd\left(a^{p/2} - 1, N\right) = 1$, then N must divide $a^{p/2} + 1$. For this example,

$$\gcd\left(a^{p/2} - 1, N\right) = \gcd\left(3^2 - 1, 20\right) = \gcd(8, 20) = 4$$
$$\gcd\left(a^{p/2} + 1, N\right) = \gcd\left(3^2 + 1, 20\right) = \gcd(10, 20) = 10$$

c

$Q = 512$. The first register has collapsed to

$$\sqrt{\frac{p}{Q}} \sum_{j=0}^{Q/p-1} |2 + jp\rangle = \frac{1}{8\sqrt{2}} \sum_{j=0}^{127} |2 + 4j\rangle$$

d

$$\frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} \omega_Q^{j\frac{Q}{p}\cdot 2} \left| j\frac{Q}{p} \right\rangle = \frac{1}{2} \sum_{j=0}^{3} (-1)^j \, |128j\rangle$$

e

The measurement only tells us that $384 = jQ/p$ for some random integer j, but if we repeat the process and take the GCD of all the results, eventually we can recover Q/p. For this example, we only need get one of $\{128, 256\}$:

$$\frac{Q}{p} = \gcd(384, 128) = \gcd(384, 256) = 128$$

Then we can recover p from Q/p:

$$p = \frac{Q}{128} = \frac{512}{128} = 4.$$

CS 498 QC Fall 2023 Wenqi He (wenqihe2)
Homework 4 Problem 4

a

- $\Rightarrow$: Suppose $\gcd(a, N) > 1$. Consider $b' \equiv b + N/\gcd(a, N) \pmod N$,

  $$ab' \equiv ab + aN/\gcd(a, N) \equiv ab + \operatorname{lcm}(a, N) \equiv ab \pmod N$$

  which means that for any b, column b and $(b + N/\gcd(a, N)) \bmod N$ are identical instead of orthogonal to each other, therefore U_a is not unitary. Therefore, if U_a is unitary, then a and N must be coprime.

- $\Leftarrow$: If a and N are coprime, then there exists an integer r such that $a^r \equiv 1 \pmod N$, i.e. a^{r-1} is the inverse of a. If $ab' \equiv ab \pmod N$, we can multiply a^{r-1} on both sides and get $b \equiv b' \pmod N$. In other words, if $b \not\equiv b' \pmod N$, then $ab \not\equiv ab' \pmod N$, which implies that

  $$\left\langle ab \bmod N \,\middle|\, ab' \bmod N \right\rangle = \delta_{bb'},$$

  therefore U_a is a unitary.

b

$$\begin{aligned}
U_a \left|\psi_\ell\right\rangle &= \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} e^{-2\pi i k\ell/p}\, U_a \left|a^k \bmod N\right\rangle = \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} e^{-2\pi i k\ell/p} \left|a^{k+1} \bmod N\right\rangle \\
&= \frac{1}{\sqrt{p}} \sum_{k=1}^{p} e^{-2\pi i (k-1)\ell/p} \left|a^k \bmod N\right\rangle = \frac{e^{2\pi i \ell/p}}{\sqrt{p}} \sum_{k=1}^{p} e^{-2\pi i k\ell/p} \left|a^k \bmod N\right\rangle \\
&= \frac{e^{2\pi i \ell/p}}{\sqrt{p}} \sum_{k=0}^{p-1} e^{-2\pi i k\ell/p} \left|a^k \bmod N\right\rangle = e^{2\pi i \ell/p} \left|\psi_\ell\right\rangle
\end{aligned}$$

c

$$\begin{aligned}
\frac{1}{\sqrt{p}} \sum_{\ell=0}^{p-1} \left|\psi_\ell\right\rangle &= \frac{1}{p} \sum_{\ell=0}^{p-1} \sum_{k=0}^{p-1} e^{-2\pi i k\ell/p} \left|a^k \bmod N\right\rangle \\
&= \frac{1}{p} \sum_{k=0}^{p-1} \left(\sum_{\ell=0}^{p-1} e^{-2\pi i k\ell/p} \right) \left|a^k \bmod N\right\rangle
\end{aligned}$$

If $k \neq 0$, the sum of the coefficients vanishes. If $k = 0$, the sum equals p. Therefore,

$$\frac{1}{\sqrt{p}} \sum_{\ell=0}^{p-1} \left|\psi_\ell\right\rangle = \frac{1}{p} \cdot p \left|1\right\rangle = \left|1\right\rangle$$

d

As in Problem 2, we prepare the superposition with $H^{\otimes n}$, which gives us

$$\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|1\rangle = \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle\left(\frac{1}{\sqrt{p}}\sum_{\ell=0}^{p-1}|\psi_\ell\rangle\right) = \frac{1}{\sqrt{2^t p}}\sum_{\ell=0}^{p-1}\sum_{j=0}^{2^t-1}|j\rangle|\psi_\ell\rangle$$

After applying the controlled powers of U_a, the t ancilla qubits are in state

$$\frac{1}{\sqrt{2^t p}}\sum_{\ell=0}^{p-1}\sum_{j=0}^{2^t-1}e^{2\pi ij\ell/p}|j\rangle = \frac{1}{\sqrt{2^t p}}\sum_{\ell=0}^{p-1}\sum_{j=0}^{2^t-1}\omega^{2^t j\ell/p}|j\rangle$$

After applying (inverse) QFT_{2^t}, the state becomes

$$\frac{1}{\sqrt{2^t p}}\sum_{\ell=0}^{p-1}\sum_{k=0}^{2^t-1}\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}\omega^{j(2^t\ell/p-k)}|k\rangle$$

As before, the innermost sum is only non-zero when $2^t\ell/p-k \equiv 0 \pmod{2^t}$, and since $0 \leq \ell < p$, $0 \leq 2^t\ell/p < 2^t$, $0 \leq k < 2^t$, $-2^t < 2^t\ell/p - k < 2^t$, this is only possible when $k = 2^t\ell/p$. The state can be simplified to

$$\frac{1}{\sqrt{2^t p}}\sum_{\ell=0}^{p-1}\sqrt{2^t}\left|2^t\frac{\ell}{p}\right\rangle = \frac{1}{\sqrt{p}}\sum_{\ell=0}^{p-1}\left|2^t\frac{\ell}{p}\right\rangle$$

When we measure the ancilla qubits, we get $b = 2^t\ell/p$ for some uniformly random ℓ.

CS 498 QC Fall 2023 Wenqi He (wenqihe2)
Homework 3 Problem 1

a

The joint state of the first n qubits can be written as

$$\begin{aligned}
|\psi\rangle &= \sum_{x\in\{0,1\}^n} c_x |x\rangle = \sum_{x\in\{0,1\}^{n-1}} a_x |0\rangle \otimes |x\rangle + \sum_{x\in\{0,1\}^{n-1}} b_x |1\rangle \otimes |x\rangle \\
&= |0\rangle \otimes \sum_{x\in\{0,1\}^{n-1}} a_x |x\rangle + |1\rangle \otimes \sum_{x\in\{0,1\}^{n-1}} b_x |x\rangle \\
&= \alpha |0\rangle \otimes \left(\frac{1}{\alpha} \sum_{x\in\{0,1\}^{n-1}} a_x |x\rangle\right) + \beta |1\rangle \otimes \left(\frac{1}{\beta} \sum_{x\in\{0,1\}^{n-1}} b_x |x\rangle\right)
\end{aligned}$$

where

$$\alpha := \sqrt{\sum_{x\in\{0,1\}^{n-1}} |a_x|^2}, \quad \beta := \sqrt{\sum_{x\in\{0,1\}^{n-1}} |b_x|^2}, \quad |\alpha|^2 + |\beta|^2 = 1$$

Since we only care about the first qubit, let's just simply write the state as

$$|\psi\rangle = \alpha |0\rangle |\psi_0\rangle + \beta |1\rangle |\psi_1\rangle$$

With the original circuit, if we measure the first qubit, we get 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$. The post-measurement state is $|0\rangle |\psi_0\rangle$ if the outcome is 0 and $|1\rangle |\psi_1\rangle$ if the outcome is 1.

With the new circuit, after applying CNOT, the joint state of all $n+1$ qubits is

$$\alpha |0\rangle |\psi_0\rangle |0\rangle + \beta |1\rangle |\psi_1\rangle |1\rangle .$$

If we measure the auxiliary qubit, we still get 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$. The post-measurement state of the first n qubits is still $|0\rangle |\psi_0\rangle$ and $|1\rangle |\psi_1\rangle$ for outcomes 0 and 1 respectively.

b

Suppose there are no other measurement after t, the entire circuit for the first n qubits after the CNOT is just a $n \times n$ unitary U, and the final state is either $U(|0\rangle |\psi_0\rangle)$ or $U(|1\rangle |\psi_1\rangle)$. If we don't measure at t, the final state before measurement will be

$$\alpha U(|0\rangle |\psi_0\rangle) |0\rangle + \beta U(|1\rangle |\psi_1\rangle) |1\rangle ,$$

If we then measure the auxiliary qubit, we still get 0 with probability $|\alpha|^2$ and 1 with probability $|b|^2$. The post-measurement state is still $U(|0\rangle |\psi_0\rangle)$ for the first n qubits if the outcomes is 0 and $U(|1\rangle |\psi_1\rangle)$ if the outcome is 1.

c

To prove that the 3-qubit gate "controlled-U" is a unitary, we only need to prove that it preserves length. To that end, we only need to show that given any valid quantum state (i.e. unit vector) the output is still a valid quantum state. Suppose we have 3 qubits whose joint state is

$$|\psi\rangle = \sum_{x\in\{0,1\}^3} c_x |x\rangle = \sum_{x\in\{0,1\}^2} a_x |0\rangle |x\rangle + \sum_{x\in\{0,1\}^2} b_x |1\rangle |x\rangle ,$$

where

$$\sum_{x\in\{0,1\}^2} |a_x|^2 + \sum_{x\in\{0,1\}^2} |b_x|^2 = 1$$

After applying the "controlled-U", the state becomes

$$|\psi'\rangle = \sum_{x\in\{0,1\}^2} a_x |0\rangle |x\rangle + \sum_{x\in\{0,1\}^2} b_x |1\rangle U |x\rangle ,$$

and its squared norm is

$$\begin{aligned}
\langle \psi' \mid \psi' \rangle &= \left(\sum_{x\in\{0,1\}^2} \overline{a_x} \langle 0| \langle x| + \sum_{x\in\{0,1\}^2} \overline{b_x} \langle 1| \langle x| U^\dagger \right) \left(\sum_{x\in\{0,1\}^2} a_x |0\rangle |x\rangle + \sum_{x\in\{0,1\}^2} b_x |1\rangle U |x\rangle \right) \\
&= \sum_{x,x'\in\{0,1\}^2} \overline{a_x} a_{x'} \langle 0 \mid 0\rangle \langle x \mid x' \rangle + \sum_{x,x'\in\{0,1\}^2} \overline{b_x} b_{x'} \langle 1 \mid 1 \rangle \langle x| U^\dagger U |x'\rangle \\
&= \sum_{x,x'\in\{0,1\}^2} \overline{a_x} a_{x'} \langle 0 \mid 0\rangle \langle x \mid x' \rangle + \sum_{x,x'\in\{0,1\}^2} \overline{b_x} b_{x'} \langle 1 \mid 1 \rangle \langle x \mid x' \rangle \\
&= \sum_{x\in\{0,1\}^2} \overline{a_x} a_x \langle 0 \mid 0\rangle \langle x \mid x \rangle + \sum_{x\in\{0,1\}^2} \overline{b_x} b_x \langle 1 \mid 1 \rangle \langle x \mid x \rangle \\
&= \sum_{x,x'\in\{0,1\}^2} |a_x|^2 + |b_x|^2 = 1
\end{aligned}$$

We eliminated cross terms at the second step because $|0\rangle |x\rangle$ and $|1\rangle |x'\rangle$ are orthogonal.

d

Since "controlled-U" is a 3×3 unitary, the entire circuit for the first n qubits after the CNOT is still a $n \times n$ unitary, so the argument in (b) still applies, i.e., the final state is still

$$\begin{aligned}
|\phi\rangle &= \alpha U (|0\rangle |\psi_0\rangle) |0\rangle + \beta U (|1\rangle |\psi_1\rangle) |1\rangle \\
&= \alpha \left(\sum_{x\in\{0,1\}^n} a_x |x\rangle \right) \otimes |0\rangle + \beta \left(\sum_{x\in\{0,1\}^n} b_x |x\rangle \right) \otimes |1\rangle ,
\end{aligned}$$

for certain a_x's and b_x's. If we measure the i-th qubit, we'll get a classical bit c with probability

$$\sum_{x\in\{0,1\}^2,\ x_i=c} |\alpha|^2 |a_x|^2 + \sum_{x\in\{0,1\}^2,\ x_i=c} |\beta|^2 |b_x|^2 = \sum_{x\in\{0,1\}^2,\ x_i=c} |\alpha|^2 |a_x|^2 + |\beta|^2 |b_x|^2$$

If we measure the $(n+1)$-th qubit first, the state of the first n qubits collapses into

$$\sum_{x \in \{0,1\}^n} a_x \left|x\right\rangle$$

with probability $|\alpha|^2$. If we then measure the i-th qubit, we'll get c with probability

$$\sum_{x \in \{0,1\}^n,\ x_i = c} |a_x|^2 .$$

Similarly, the state collapses into

$$\sum_{x \in \{0,1\}^n} b_x \left|x\right\rangle$$

with probability $|\beta|^2$, and we get c for the i-th qubit with probability

$$\sum_{x \in \{0,1\}^n,\ x_i = c} |b_x|^2 .$$

Overall, the total probability of measuring c for the i-th qubit is still

$$|\alpha|^2 \sum_{x \in \{0,1\}^n,\ x_i = c} |a_x|^2 + |\beta|^2 \sum_{x \in \{0,1\}^n,\ x_i = c} |b_x|^2 = \sum_{x \in \{0,1\}^n,\ x_i = c} |\alpha|^2 |a_x|^2 + |\beta|^2 |b_x|^2$$

e

It depends on whether or not we intend to create two "branches" of reality that don't interfere with each other. With the CNOT at time t, even though we have the freedom to not measure the $(n+1)$-th qubit in the end, its entanglement with the first n qubits separates the two "branches" in the superposition (the one where the last qubit is $\left|0\right\rangle$ and the one where it's $\left|1\right\rangle$), which has the same effect as measurement. Without the CNOT, the two "branches" could still interfere with each other after the rest of the circuit is applied. The final state in this case would be

$$\begin{aligned}
\left|\phi'\right\rangle &= \alpha U\left(\left|0\right\rangle \left|\psi_0\right\rangle\right) + \beta U\left(\left|1\right\rangle \left|\psi_1\right\rangle\right) \\
&= \alpha \left(\sum_{x \in \{0,1\}^n} a_x \left|x\right\rangle \right) + \beta \left(\sum_{x \in \{0,1\}^n} b_x \left|x\right\rangle \right) \\
&= \sum_{x \in \{0,1\}^n} \left(\alpha a_x + \beta b_x\right) \left|x\right\rangle
\end{aligned}$$

Using the fact that

$$|a+b|^2 = (\overline{a}+\overline{b})(a+b) = \overline{a}a + \overline{a}b + \overline{b}a + \overline{b}b = |a|^2 + |b|^2 + \Re(a\overline{b}),$$

the probability of reading c when measuring the i-th qubit is

$$\sum_{x \in \{0,1\}^n,\ x_i = c} |\alpha a_x + \beta b_x|^2 = \sum_{x \in \{0,1\}^n,\ x_i = c} |\alpha|^2 |a_x|^2 + |\beta|^2 |b_x|^2 + \Re(\alpha a_x \overline{\beta b_x}),$$

The extra term $\Re(\alpha a_x \overline{\beta b_x})$, which might be nonzero, is the result of interference.

CS 498 QC Fall 2023 Wenqi He (wenqihe2)

Homework 3 Problem 2

(i) Create a circuit implementing Deutsch's algorithm and draw it.

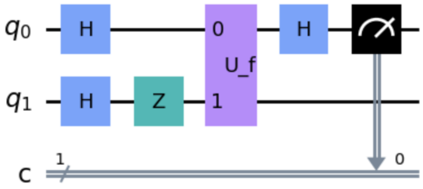
[3]:

```
from qiskit import QuantumCircuit

circ = QuantumCircuit(2, 1)
circ.h(0)
circ.h(1)
circ.z(1)
U_f(circ, [0, 1])
circ.h(0)
circ.measure([0], [0])

circ.draw()
```

[3]:



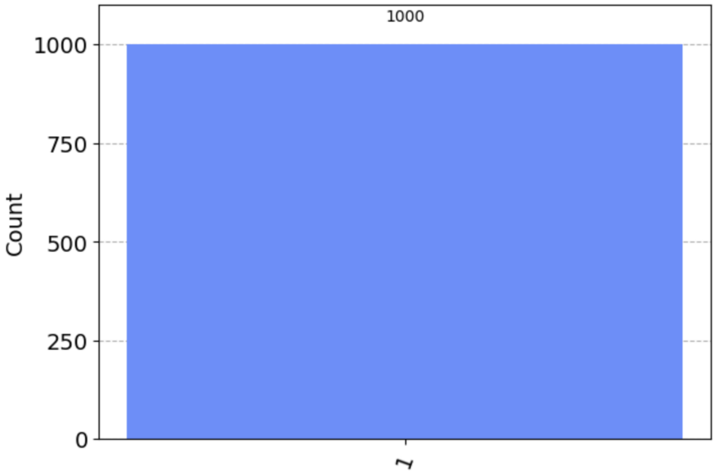
(ii) Execute it with 1000 shots using IBM's 'qasm simulator' and plot your results, and determine whether the function is constant or balanced.

[4]:

```
from qiskit import Aer, execute
from qiskit.visualization import plot_histogram

backend_sim = Aer.get_backend('qasm_simulator')
sim = execute(circ, backend_sim, shots=1000)
sim_result = sim.result()
counts = sim_result.get_counts(circ)
plot_histogram(counts)
```

[4]:



The result is always $|1\rangle$, which means that the state of the first qubit is $\pm|-\rangle$ before the last Hadamard gate is applied. According to the algorithm, the function is balanced.

CS 498 QC Fall 2023 Wenqi He (wenqihe2)

Homework 3 Problem 3

a

We can divide the domain, which contains 2^n strings, into equivalent classes of size 4, each of which maps to a single output, so the maximum number of output values is the number of equivalent classes, which is 2^{n-2}

b

For each trial, repeat for $n-2$ times:

1. Prepare n input qubits and n output qubits in state $|0\rangle$.
2. Apply $H^{\otimes n}$ to the input qubits
3. Apply U_f, the quantum circuit that implements f.
4. Measure the output qubits.
5. Apply a second $H^{\otimes n}$ to the input qubits.
6. Measure the input qubits, resulting in a vector $s \in \mathbb{F}_2{}^n$.

Repeat until we collect $n-2$ linearly independent vectors. Each vector $s \in \mathbb{F}_2{}^n$ encodes a linear equation $s \cdot x = 0$. The dimension of the subspace spanned by the solutions is $n-(n-2)=2$, so there are $2^2=4$ solutions, and the three non-zero ones are K, L and $K+L$ (in any order).

c

The joint state of the $2n$ qubits after Step 2 is

$$\left(H^{\otimes n}|0\rangle^{\otimes n}\right) \otimes |0\rangle^{\otimes n} = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)^{\otimes n} \otimes |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |0\rangle^{\otimes n}$$

After Step 3, the state is

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |f(x)\rangle^{\otimes n}$$

After Step 4, suppose the result of the measurement is $f(x^*)$ for some x^*, the state collapses into

$$\frac{1}{2}\left(|x^*\rangle + |x^*+K\rangle + |x^*+L\rangle + |x^*+K+L\rangle\right) \otimes |f(x^*)\rangle^{\otimes n}$$

Applying $H^{\otimes n}$ to $|x\rangle$ results in

$$\begin{aligned}H^{\otimes n}|x\rangle &= H|x_{n-1}\rangle \otimes \cdots \otimes H|x_0\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{(-1)^{x_{n-1}}}{\sqrt{2}}|1\rangle\right) \otimes \cdots \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{(-1)^{x_0}}{\sqrt{2}}|1\rangle\right)\\ &= \frac{1}{\sqrt{2^n}} \sum_{s\in\{0,1\}^n} \prod_{i=0}^{n-1} (-1)^{x_i s_i}|s\rangle = \frac{1}{\sqrt{2^n}} \sum_{s\in\{0,1\}^n} (-1)^{\sum_{i=0}^{n-1} x_i s_i}|s\rangle\\ &= \frac{1}{\sqrt{2^n}} \sum_{s\in\{0,1\}^n} (-1)^{s\cdot x}|s\rangle\end{aligned}$$

and the sum over such terms goes all the way to the inside,

$$\sum_x H^{\otimes n}|x\rangle = \sum_x \frac{1}{\sqrt{2^n}} \sum_{s\in\{0,1\}^n} (-1)^{s\cdot x}|s\rangle = \frac{1}{\sqrt{2^n}} \sum_{s\in\{0,1\}^n} \left(\sum_x (-1)^{s\cdot x}\right)|s\rangle$$

After Step 5, the joint state of the input qubits is

$$\begin{aligned}|\psi\rangle &= \frac{1}{2}\left(H^{\otimes n}|x^*\rangle + H^{\otimes n}|x^*+K\rangle + H^{\otimes n}|x^*+L\rangle + H^{\otimes n}|x^*+K+L\rangle\right)\\ &= \frac{1}{\sqrt{2^{n+2}}} \sum_{s\in\{0,1\}^n} \left[(-1)^{s\cdot x^*} + (-1)^{s\cdot(x^*+K)} + (-1)^{s\cdot(x^*+L)} + (-1)^{s\cdot(x^*+K+L)}\right]|s\rangle\\ &= \frac{1}{\sqrt{2^{n+2}}} \sum_{s\in\{0,1\}^n} (-1)^{s\cdot x^*}\left[1 + (-1)^{s\cdot K} + (-1)^{s\cdot L} + (-1)^{s\cdot(K+L)}\right]|s\rangle\\ &= \frac{1}{\sqrt{2^{n+2}}} \sum_{s\in\{0,1\}^n} (-1)^{s\cdot x^*}\left[1 + (-1)^{s\cdot K}\right]\left[1 + (-1)^{s\cdot L}\right]|s\rangle\end{aligned}$$

We can pull out $(-1)^{s\cdot x^*}$ in the last step because $(-1)^{a+b} = (-1)^a(-1)^b$ for $a, b \in \mathbb{F}_2$. The only terms that remain are those where $s\cdot K = s\cdot L = 0$,

$$|\psi\rangle = \frac{1}{\sqrt{2^{n-2}}} \sum_{s\in\{0,1\}^n,\ s\cdot K = s\cdot L = 0} (-1)^{s\cdot x}|s\rangle$$

We now have 2^{n-2} uniformly distributed vectors. Suppose we have already collected i linearly independent vectors, at most 2^i out of the 2^{n-2} possible vectors will be within the span of the previous i vectors, so the probability of finding the $(i+1)$-th linearly independent vector is at least $1 - 2^i/2^{n-2}$. The probability that after $n-2$ iterations, we find all $n-2$ vectors we need is

$$\begin{aligned}P &\geq \prod_{i=0}^{n-3}\left(1 - \frac{2^i}{2^{n-2}}\right) = \frac{1}{2}\prod_{i=0}^{n-4}\left(1 - \frac{2^i}{2^{n-2}}\right)\\ &\geq \frac{1}{2}\left(1 - \sum_{i=0}^{n-4}\frac{2^i}{2^{n-2}}\right) = \frac{1}{2}\left(1 - \frac{2^{n-3}-1}{2^{n-2}}\right)\\ &\geq \frac{1}{2}\left(1 - \frac{1}{2}\right) = \frac{1}{4}\end{aligned}$$

The expected number of trials until success is $1/P \leq 4$, and we perform $n-2 < n$ queries in each trials, so in total, we can expect to perform at most $4n$ queries.

d

Nothing really changes, except that we now only need $n-r$ linearly independent vectors/equations and we could now use only $n-r$ iterations/queries in each trial to achieve the same lower bound for the probability of success after one trial.

Proof

For convenience, we'll refer to the r secrets as $L^{(0)}, \dots, L^{(r-1)}$.

With r secrets, after measuring the output of U_f, if we get $f(x^*)$ for some x^*, the post-measurement state is a superposition of states representing all possible linear combinations of the r secrets plus x^*:

$$\frac{1}{\sqrt{2^r}} \sum_{x \in \{0,1\}^r} \left| x^* + \sum_{i=0}^{r-1} x_i L^{(i)} \right\rangle$$

After applying the second $H^{\otimes n}$,

$$\begin{aligned}
|\psi\rangle &= \frac{1}{\sqrt{2^r}} \sum_{x \in \{0,1\}^r} H^{\otimes n} \left| x^* + \sum_{i=0}^{r-1} x_i L^{(i)} \right\rangle \\
&= \frac{1}{\sqrt{2^r}} \sum_{x \in \{0,1\}^r} \frac{1}{\sqrt{2^n}} \sum_{s \in \{0,1\}^n} (-1)^{s \cdot \left(x^* + \sum_{i=0}^{r-1} x_i L^{(i)} \right)} |s\rangle \\
&= \frac{1}{\sqrt{2^{n+r}}} \sum_{s \in \{0,1\}^n} (-1)^{s \cdot x^*} \sum_{x \in \{0,1\}^r} (-1)^{\sum_{i=0}^{r-1} x_i s \cdot L^{(i)}} |s\rangle \\
&= \frac{1}{\sqrt{2^{n+r}}} \sum_{s \in \{0,1\}^n} (-1)^{s \cdot x^*} \prod_{i=0}^{r-1} \left[1 + (-1)^{s \cdot L^{(i)}} \right] |s\rangle
\end{aligned}$$

The only basis states $|s\rangle$ that remain must satisfy

$$s \cdot L^{(0)} = s \cdot L^{(1)} = \cdots = s \cdot L^{(r-1)} = 0.$$

Therefore, the state can be simplified as

$$|\psi\rangle = \frac{1}{\sqrt{2^{n+r}}} \sum_{s \in \{0,1\}^n, \forall i. s \cdot L^{(i)} = 0} (-1)^{s \cdot x^*} 2^r |s\rangle = \frac{1}{\sqrt{2^{n-r}}} \sum_{s \in \{0,1\}^n, \forall i. s \cdot L^{(i)} = 0} (-1)^{s \cdot x^*} |s\rangle$$

With r secrets, we are now sampling from 2^{n-r} instead of 2^{n-2} uniformly distributed vectors. Since we only need to reduce the dimension of the solution subspace to r, we only need to collect $n-r$ linearly independent equations. Thus, we could modify the algorithm to only repeat $n-r$

iterations in each trial and still achieve

$$\begin{aligned} P(\text{success after one trial}) &\geq \prod_{i=0}^{n-r-1}\left(1-\frac{2^i}{2^{n-r}}\right) = \frac{1}{2}\prod_{i=0}^{n-r-2}\left(1-\frac{2^i}{2^{n-r}}\right) \\ &\geq \frac{1}{2}\left(1-\sum_{i=0}^{n-r-2}\frac{2^i}{2^{n-r}}\right) = \frac{1}{2}\left(1-\frac{2^{n-r-1}-1}{2^{n-r}}\right) \\ &\geq \frac{1}{2}\left(1-\frac{1}{2}\right) = \frac{1}{4} \end{aligned}$$

The expected number of trials until success is still at most 4, and the expected number of queries to f is at most $4(n-r)$.

CS 498 QC Fall 2023 Wenqi He (wenqihe2)

Homework 2 Problem 1

a

The state can be written as

$$|\psi\rangle = \frac{1}{\sqrt{2}}\,|a_0\rangle\,\langle a_0\,|\,0\rangle\,|0\rangle + \frac{1}{\sqrt{2}}\,|a_1\rangle\,\langle a_1\,|\,0\rangle\,|0\rangle + \frac{1}{\sqrt{2}}\,|a_0\rangle\,\langle a_0\,|\,1\rangle\,|1\rangle + \frac{1}{\sqrt{2}}\,|a_1\rangle\,\langle a_1\,|\,1\rangle\,|1\rangle$$

Alice measures $|a_i\rangle$, where $i \in \{0, 1\}$, with probability

$$\left|\frac{1}{\sqrt{2}}\,\langle a_i\,|\,0\rangle\right|^2 + \left|\frac{1}{\sqrt{2}}\,\langle a_i\,|\,1\rangle\right|^2 = \frac{1}{2}\left(|\langle a_i\,|\,0\rangle|^2 + |\langle a_i\,|\,1\rangle|^2\right) = \frac{1}{2}$$

b

If Alice measures $|a_i\rangle$, the post-measurement state is

$$\begin{aligned}
|\phi\rangle &= \frac{\left(\frac{1}{\sqrt{2}}\,|a_i\rangle\,\langle a_i\,|\,0\rangle\,|0\rangle + \frac{1}{\sqrt{2}}\,|a_i\rangle\,\langle a_i\,|\,1\rangle\,|1\rangle\right)}{\frac{1}{\sqrt{2}}} \\
&= |a_i\rangle\,\langle a_i\,|\,0\rangle\,|0\rangle + |a_i\rangle\,\langle a_i\,|\,1\rangle\,|1\rangle \\
&= |a_i\rangle \otimes (\langle a_i\,|\,0\rangle\,|0\rangle + \langle a_i\,|\,1\rangle\,|1\rangle) = |a_i\rangle \otimes \left(\overline{\langle 0\,|\,a_i\rangle}\,|0\rangle + \overline{\langle 1\,|\,a_i\rangle}\,|1\rangle\right) \\
&= |a_i\rangle \otimes |a_i\rangle^*
\end{aligned}$$

c

If Alice measures $|a_i\rangle$, the probability that Bob measures $|b_j\rangle$ is

$$P\left(b_j \mid a_i\right) = |\langle b_j\,|\,a_i\rangle^*|^2 = |\langle a_i\,|\,0\rangle\,\langle b_j\,|\,0\rangle + \langle a_i\,|\,1\rangle\,\langle b_j\,|\,1\rangle|^2$$

d

The state can also be written as

$$|\psi\rangle = \frac{1}{\sqrt{2}}\,|0\rangle\,|b_0\rangle\,\langle b_0\,|\,0\rangle + \frac{1}{\sqrt{2}}\,|0\rangle\,|b_1\rangle\,\langle b_1\,|\,0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,|b_0\rangle\,\langle b_0\,|\,1\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,|b_1\rangle\,\langle b_1\,|\,1\rangle$$

Bob measures $|b_j\rangle$ with probability $\frac{1}{2}$, and the post-measurement state is

$$|\phi\rangle = (\langle b_j\,|\,0\rangle\,|0\rangle + \langle b_j\,|\,1\rangle\,|1\rangle) \otimes |b_j\rangle$$

The probability that Alice then measures $|a_i\rangle$ is

$$|\langle b_j\,|\,0\rangle\,\langle a_i\,|\,0\rangle + \langle b_j\,|\,1\rangle\,\langle a_i\,|\,1\rangle|^2$$

In both scenarios, the joint probability that Alice measures $|a_i\rangle$ and Bob measures $|b_j\rangle$ is

$$P(a_i, b_j) = \frac{1}{2}\,|\langle a_i\,|\,0\rangle\,\langle b_j\,|\,0\rangle + \langle a_i\,|\,1\rangle\,\langle b_j\,|\,1\rangle|^2$$

e

We have shown that for any a_i and b_i, $P(a_i) = P(b_j) = \dfrac{1}{2}$ and $P(a_i \mid b_j) = P(b_j \mid a_i)$, so the probability that Bob measures $|b_j\rangle$ after Alice measures her qubit in some basis $\{a_0, a_1\}$ is

$$P(a_0)P(b_j \mid a_0) + P(a_1)P(b_j \mid a_1) = P(b_j)P(a_0 \mid b_j) + P(b_j)P(a_1 \mid b_j) = P(b_j) = \frac{1}{2}$$

That is, Bob can't tell in which basis Alice has made the measurement, or whether Alice has made any measuremnt at all.

CS 498 QC Fall 2023 Wenqi He (wenqihe2)
Homework 2 Problem 2

a

We first prove the deterministic case: Suppose there is a strategy that's guaranteed to win, that is,

$$\begin{aligned} a(0) \oplus b(0) \oplus c(0) &= 0 \vee 0 \vee 0 = 0 \\ a(1) \oplus b(1) \oplus c(0) &= 1 \vee 1 \vee 0 = 1 \\ a(1) \oplus b(0) \oplus c(1) &= 1 \vee 0 \vee 1 = 1 \\ a(0) \oplus b(1) \oplus c(1) &= 0 \vee 1 \vee 1 = 1 \end{aligned}$$

If we $\oplus$ the above equations together, we get $0 = 1$, which is a contradiction, which means that there is no deterministic strategy that gives 4 correct answers. However, we can devise a strategy that gets 3 answers correct: For example, if Alice and Bob always respond with 0 and Charlie always responds with 1, the answer would be correct except for 000. Thus, the optimal winning probability is $3/4$.

For the randomized case, we can model the strategy using a single random variable λ (if there are multiple random variables we can combine them by concatenating the bits). Given the value of λ, the strategy is deterministic, so $P(win \mid \lambda) \leq 3/4$. Therefore, the optimal winning probability of a randomized strategy is

$$\sum_{\lambda} P(\lambda) P(win \mid \lambda) \leq \frac{3}{4} \sum_{\lambda} P(\lambda) = \frac{3}{4}.$$

b

The winning probability of this strategy is 1, which is obviously optimal.

The intuition is that every measurement but the last will yield either 1 or 0, each with $1/2$ probability; the outcome of the last measurement, however, will be uniquely determined by all preceding measurements, and the answers will be correct for all questions.

It might be easier to illustrate the pattern by generalizing the setup. Suppose there are n qubits and their entangled joint state is

$$\frac{1}{\sqrt{2}} |0\rangle^{\otimes n} + \frac{c}{\sqrt{2}} |1\rangle^{\otimes n}$$

where c is a phase factor. Without loss of generality, suppose the first qubit is measured first based on the strategy. Since the strategy is symmetric for all parties, other scenarios are essentially the same. For convenience, let's use $\alpha \to \beta$ to denote the step of "receiving α and answering β". There are 4 cases for a single step, each of which preserve the entanglement but applies a different phase shift to the second amplitude:

- $0 \to 0$: The post-measurement state for the rest of the qubits is

$$\langle + \mid 0 \rangle |0\rangle^{\otimes n-1} + c \langle + \mid 1 \rangle |1\rangle^{\otimes n-1} = \frac{1}{\sqrt{2}} |0\rangle^{\otimes n-1} + \frac{c}{\sqrt{2}} |1\rangle^{\otimes n-1}$$

- $0 \to 1$: The post-measurement state for the rest of the qubits is

$$\langle - \,|\, 0\rangle \left|0\right\rangle^{\otimes n-1} + c \langle - \,|\, 1\rangle \left|1\right\rangle^{\otimes n-1} = \frac{1}{\sqrt{2}} \left|0\right\rangle^{\otimes n-1} - \frac{c}{\sqrt{2}} \left|1\right\rangle^{\otimes n-1}$$

- $1 \to 0$: The post-measurement state for the rest of the qubits is

$$\langle i \,|\, 0\rangle \left|0\right\rangle^{\otimes n-1} + c \langle i \,|\, 1\rangle \left|1\right\rangle^{\otimes n-1} = \frac{1}{\sqrt{2}} \left|0\right\rangle^{\otimes n-1} - \frac{ic}{\sqrt{2}} \left|1\right\rangle^{\otimes n-1}$$

- $1 \to 1$: The post-measurement state for the rest of the qubits is

$$\langle -i \,|\, 0\rangle \left|0\right\rangle^{\otimes n-1} + c \langle -i \,|\, 1\rangle \left|1\right\rangle^{\otimes n-1} = \frac{1}{\sqrt{2}} \left|0\right\rangle^{\otimes n-1} + \frac{ic}{\sqrt{2}} \left|1\right\rangle^{\otimes n-1}$$

Let's now analyze all possibilities:

- Question 000:
  - If the first two steps are $\{0 \to \beta, 0 \to \beta\}$, the final state is

    $$\frac{1}{\sqrt{2}} \left|0\right\rangle + \frac{1}{\sqrt{2}} \left|1\right\rangle = \left|+\right\rangle,$$

    so the last step is $0 \to 0$, and the answer is $\beta \oplus \beta \oplus 0 = 0 = 0 \vee 0 \vee 0$.
  - If the first two steps are $\{0 \to \beta, 0 \to \neg\beta\}$, the final state is

    $$\frac{1}{\sqrt{2}} \left|0\right\rangle - \frac{1}{\sqrt{2}} \left|1\right\rangle = \left|-\right\rangle,$$

    so the last step is $0 \to 1$, and the answer is $\beta \oplus \neg\beta \oplus 1 = 0 = 0 \vee 0 \vee 0$.

- Question 110, 101, or 011:
  - If the first two steps are $\{1 \to \beta, 1 \to \beta\}$, the final state is

    $$\frac{1}{\sqrt{2}} \left|0\right\rangle - \frac{1}{\sqrt{2}} \left|1\right\rangle = \left|-\right\rangle,$$

    so the last step is $0 \to 1$, and the answer is $\beta \oplus \beta \oplus 1 = 1 = 1 \vee 1 \vee 0$.
  - If the first two steps are $\{1 \to \beta, 1 \to \neg\beta\}$, the final state is

    $$\frac{1}{\sqrt{2}} \left|0\right\rangle + \frac{1}{\sqrt{2}} \left|1\right\rangle = \left|+\right\rangle,$$

    so the last step is $0 \to 0$, and the answer is $\beta \oplus \neg\beta \oplus 0 = 1 = 1 \vee 1 \vee 0$.
  - If the first two steps are $\{\alpha \to \beta, \neg\alpha \to \beta\}$, the final state is

    $$\frac{1}{\sqrt{2}} \left|0\right\rangle - \frac{i}{\sqrt{2}} \left|1\right\rangle = \left|-i\right\rangle,$$

    so the last step is $0 \to 1$, and the answer is $\beta \oplus \beta \oplus 1 = 1 = \alpha \vee \neg\alpha \vee 0$.
  - If the first two steps are $\{\alpha \to \beta, \neg\alpha \to \neg\beta\}$, the final state is

    $$\frac{1}{\sqrt{2}} \left|0\right\rangle + \frac{i}{\sqrt{2}} \left|1\right\rangle = \left|i\right\rangle,$$

    so the last step is $0 \to 0$, and the answer is $\beta \oplus \neg\beta \oplus 0 = 1 = \alpha \vee \neg\alpha \vee 0$.

In all cases, the last person to respond is guaranteed to produce the correct answer.

CS 498 QC Fall 2023 Wenqi He (wenqihe2)
Homework 2 Problem 3

The entangled state can be written as

$$\begin{aligned}
|\theta\rangle &= \frac{1}{\sqrt{3}}|00\rangle - \frac{1}{\sqrt{6}}|01\rangle + \frac{1}{\sqrt{6}}|10\rangle + \frac{1}{\sqrt{3}}|11\rangle \\
&= \frac{1}{\sqrt{2}}\left(\sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle\right)\otimes|0\rangle + \frac{1}{\sqrt{2}}\left(-\sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle\right)\otimes|1\rangle \\
&= \frac{1}{\sqrt{2}}R|0\rangle\otimes|0\rangle + \frac{1}{\sqrt{2}}R|1\rangle\otimes|1\rangle
\end{aligned}$$

where

$$R = \begin{pmatrix} \sqrt{\frac{2}{3}} & -\sqrt{\frac{1}{3}} \\ \sqrt{\frac{1}{3}} & \sqrt{\frac{2}{3}} \end{pmatrix}$$

To repair the EPR state, Alice only needs to invert the rotation on her qubit, by applying

$$R^{-1} = R^{\dagger} = \begin{pmatrix} \sqrt{\frac{2}{3}} & \sqrt{\frac{1}{3}} \\ -\sqrt{\frac{1}{3}} & \sqrt{\frac{2}{3}} \end{pmatrix},$$

which will recover the Bell state:

$$\left(R^{-1}\otimes I\right)|\theta\rangle = \frac{1}{\sqrt{2}}R^{-1}R|0\rangle\otimes|0\rangle + \frac{1}{\sqrt{2}}R^{-1}R|1\rangle\otimes|1\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

Now Alice and Bob can proceed with the original teleportation protocol.

CS 498 QC Fall 2023 Wenqi He (wenqihe2)

Homework 2 Problem 4

Let's call Alice's qubit A, Carol's qubit C, the qubit owned by Bob and entangled with A B_A, and the other qubit owned by Bob and entangled C B_C. We can use the following protocol:

```
BOB:
  1. Apply the CNOT gate, using $B_A$ as the control gate and $B_C$ as the target gate.
  2. Measure $B_C$, resulting in a classical bit $b_c$.
  3. Apply the Hadamard gate to $B_A$
  4. Measure $B_A$, resulting in a classical bit $b_a$.
  5. Send $b_c b_a$ to Carol.

CAROL:
  Upon receiving classical bits $b_c b_a$:
      If $b_c = 1$, apply the X gate.
      If $b_a = 1$, apply the Z gate.
```

Proof of Correctness

The initial joint state of A, B_A, B_C and C is:

$$\left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) = \frac{1}{2}|0000\rangle + \frac{1}{2}|0011\rangle + \frac{1}{2}|1100\rangle + \frac{1}{2}|1111\rangle$$

After Bob applies the local CNOT, the state becomes

$$\frac{1}{2}|0000\rangle + \frac{1}{2}|0011\rangle + \frac{1}{2}|1110\rangle + \frac{1}{2}|1101\rangle$$

After Bob measures $b_c \in \{0, 1\}$, the the joint state of the A, B_A and C becomes:

$$\frac{1}{\sqrt{2}}|00b_c\rangle + \frac{1}{\sqrt{2}}|11\neg b_c\rangle$$

After Bob applies the Hadamard gate to B_A, the state becomes:

$$\frac{1}{2}|00b_c\rangle + \frac{1}{2}|01b_c\rangle + \frac{1}{2}|10\neg b_c\rangle - \frac{1}{2}|11\neg b_c\rangle$$

After Bob measures $b_a \in \{0, 1\}$, the joint state of A and C becomes:

$$\frac{1}{\sqrt{2}}|0b_c\rangle + \frac{(-1)^{b_a}}{\sqrt{2}}|1\neg b_c\rangle$$

Upon receiving Bob's message, Carol will adjust the state to the Bell state:

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

CS 498 QC Fall 2023 Wenqi He (wenqihe2)

Homework 1 Problem 1

a

C should be the norm of $\| |\phi\rangle \| = \sqrt{3 \cdot 3 + (-5i) \cdot (5i)} = \sqrt{9 + 25} = \sqrt{34}$

b

$$\begin{aligned}
\langle i \,|\, i \rangle &= \left(\frac{1}{\sqrt{2}} \langle 0| - \frac{i}{\sqrt{2}} \langle 1| \right) \left(\frac{1}{\sqrt{2}} |0\rangle + \frac{i}{\sqrt{2}} |1\rangle \right) = \frac{1}{2} + \frac{1}{2} = 1 \\
\langle -i \,|\, -i \rangle &= \left(\frac{1}{\sqrt{2}} \langle 0| + \frac{i}{\sqrt{2}} \langle 1| \right) \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{i}{\sqrt{2}} |1\rangle \right) = \frac{1}{2} + \frac{1}{2} = 1 \\
\langle i \,|\, -i \rangle &= \left(\frac{1}{\sqrt{2}} \langle 0| - \frac{i}{\sqrt{2}} \langle 1| \right) \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{i}{\sqrt{2}} |1\rangle \right) = \frac{1}{2} - \frac{1}{2} = 0
\end{aligned}$$

The possible outcomes are $|i\rangle$ and $|-i\rangle$. The probabilities are

$$\begin{aligned}
P(|i\rangle) = |\langle i \,|\, \psi \rangle|^2 &= \left[\left(\frac{1}{\sqrt{2}} \langle 0| - \frac{i}{\sqrt{2}} \langle 1| \right) \left(\frac{3}{\sqrt{34}} |0\rangle - \frac{5i}{\sqrt{34}} |1\rangle \right) \right]^2 \\
&= \left(\frac{3}{\sqrt{68}} - \frac{5}{\sqrt{68}} \right)^2 = \left(-\frac{2}{\sqrt{68}} \right)^2 = \frac{1}{17} \\
P(|-i\rangle) = |\langle -i \,|\, \psi \rangle|^2 &= \left[\left(\frac{1}{\sqrt{2}} \langle 0| + \frac{i}{\sqrt{2}} \langle 1| \right) \left(\frac{3}{\sqrt{34}} |0\rangle - \frac{5i}{\sqrt{34}} |1\rangle \right) \right]^2 \\
&= \left(\frac{3}{\sqrt{68}} + \frac{5}{\sqrt{68}} \right)^2 = \left(\frac{8}{\sqrt{68}} \right)^2 = \frac{16}{17}
\end{aligned}$$

CS 498 QC Fall 2023 Wenqi He (wenqihe2)

Homework 1 Problem 2

a

$$|+\rangle\langle 0| = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 \end{bmatrix}$$

$$|0\rangle\langle +| = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 \end{bmatrix}$$

c

$$Q|\psi\rangle = |\phi\rangle\langle\psi\,|\,\psi\rangle = |\phi\rangle$$

$$Q|\perp\rangle = |\phi\rangle\langle\psi\,|\,\perp\rangle = \mathbf{0}$$

d

P projects a vector along the $|\psi\rangle$ direction.

e

$\mathbf{1} - 2P$ reflects a vector across the hyperplane perpendicular to $|\psi\rangle$. It is unitary because:

$$(\mathbf{1} - 2P)^\dagger(\mathbf{1} - 2P) = (\mathbf{1} - 2P)(\mathbf{1} - 2P) = (\mathbf{1} - 4P + 4P^2) = (\mathbf{1} - 4P + 4P) = \mathbf{1}$$

f

For any vector $|\psi\rangle = \sum_{i=1}^{d} \alpha_i |\psi_i\rangle$

$$|\phi\rangle = U|\psi\rangle = U\sum_{i=1}^{d}\alpha_i|\psi_i\rangle = \sum_{i=1}^{d}\alpha_i U|\psi_i\rangle = \sum_{i=1}^{d}\alpha_i\sum_{j=1}^{d}|\phi_j\rangle\langle\psi_j\,|\,\psi_i\rangle = \sum_{i=1}^{d}\alpha_i|\phi_i\rangle$$

The operator is unitary since it preserves lengths:

$$\||\phi\rangle\|^2 = \langle\phi\,|\,\phi\rangle = \sum_{i=1}^{d}|\alpha_i|^2 = \langle\psi\,|\,\psi\rangle = \||\psi\rangle\|^2$$

g

$$\mathbf{1} = |\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2| + \cdots + |\psi_d\rangle\langle\psi_d|$$

CS 498 QC Fall 2023 Wenqi He (wenqihe2)

Homework 1 Problem 3

Pass the qubit through a sequence of n measurement devices, where the k-th device measures the state in the $\left\{R_{\frac{k\pi}{2n}}\left|0\right\rangle, R_{\frac{k\pi}{2n}}\left|1\right\rangle\right\}$ basis. The qubit's state changes to $\left|1\right\rangle$ if each measurement gives $R_{\frac{k\pi}{2n}}\left|0\right\rangle$, which has probability $\cos^2\left(\frac{\pi}{2n}\right)$, so the total probability is $\cos^{2n}\left(\frac{\pi}{2n}\right)$.

CS 498 QC Fall 2023 Wenqi He (wenqihe2)

Homework 1 Problem 4

a

$$I \otimes H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

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

b

$$(I \otimes H) \left|01\right\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \left|00\right\rangle - \frac{1}{\sqrt{2}} \left|01\right\rangle$$

$$(H \otimes I) \left|01\right\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left|01\right\rangle + \frac{1}{\sqrt{2}} \left|11\right\rangle$$

$$(H \otimes H) \left|01\right\rangle = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{2} \left|00\right\rangle - \frac{1}{2} \left|01\right\rangle + \frac{1}{2} \left|10\right\rangle - \frac{1}{2} \left|11\right\rangle$$

c

For any $|a\rangle \in \mathbb{C}^d$, $|b\rangle \in \mathbb{C}^e$, $|c\rangle \in \mathbb{C}^d$, $|d\rangle \in \mathbb{C}^e$,

$$\begin{aligned}
(\langle a| \otimes \langle b|)\,(|c\rangle \otimes |d\rangle) &= \left(\sum_{i=1}^{d} \sum_{j=1}^{e} \overline{a_i b_j}\, \langle ij| \right) \left(\sum_{i'=1}^{d} \sum_{j'=1}^{e} c_{i'} d_{j'}\, |i'j'\rangle \right) \\
&= \sum_{i=1}^{d} \sum_{j=1}^{e} \sum_{i'=1}^{d} \sum_{j'=1}^{e} \overline{a_i b_j} c_{i'} d_{j'}\, \langle ij \,|\, i'j' \rangle = \sum_{i=1}^{d} \sum_{j=1}^{e} \overline{a_i b_j} c_i d_j \\
&= \left(\sum_{i=1}^{d} \overline{a_i} c_i \right) \left(\sum_{j=1}^{e} \overline{b_j} d_j \right) \\
&= \langle a \,|\, c \rangle \, \langle b \,|\, d \rangle
\end{aligned}$$

Therefore, the inner product of the (i, j)-th and (i', j')-th vectors is

$$(\langle u_i| \otimes \langle v_j|)(|u_{i'}\rangle \otimes |v_j\rangle) = \left\langle u_i \,\middle|\, u_i' \right\rangle \left\langle v_j \,\middle|\, v_j' \right\rangle = \delta_{ii'} \delta_{jj'}$$

i.e. the inner product is 0 if the two vectors are different and 1 if they are the same, which means that $|u_i\rangle \otimes |v_j\rangle$ forms a orthonormal basis.

d

The matrix component at row (i, m) and column (j, n) is

$$(\langle u_i| \otimes \langle v_m|)\; (A \otimes B)\, (|u_j\rangle \otimes |v_n\rangle) = \langle u_i|\, A \,|v_j\rangle \, \langle v_m|\, B \,|v_n\rangle$$

e

The state is not entangled because it can be factored. For example, one factorization is

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle = \left(\frac{1}{\sqrt{2^j}} \sum_{x \in \{0,1\}^j} |x\rangle \right) \left(\frac{1}{\sqrt{2^{n-j}}} \sum_{x \in \{0,1\}^{n-j}} |x\rangle \right)$$

i.e. Alice's and Bob's respective states could be $\left(\frac{1}{\sqrt{2^j}} \sum_{x \in \{0,1\}^j} |x\rangle \right)$ and $\left(\frac{1}{\sqrt{2^{n-j}}} \sum_{x \in \{0,1\}^{n-j}} |x\rangle \right)$.