CS 593/MA 592 - Intro to Quantum Computing
Spring 2024
Thursday, February 8 - Lecture 5.2

Today's scribe: Hao Wan

Agenda:

1. No-cloning theorem
2. Superdense coding
3. Bernstein-Vazirani algorithm
4. BQP ⊂ PSPACE

1 No-cloning Theorem

Theorem 1. *There does not exist a unitary operator*

$$\begin{aligned} U : \mathbb{C}^2 \otimes \mathbb{C}^2 &\longrightarrow \mathbb{C}^2 \otimes \mathbb{C}^2 \\ |\psi\rangle \otimes |0\rangle &\longmapsto |\psi\rangle \otimes |\psi\rangle \end{aligned}$$

Proof. Suppose there exists such a U, we will show it cannot be linear. Observe that

$$U(|\psi_1\rangle \otimes |0\rangle) + U(|\psi_2\rangle \otimes |0\rangle) = |\psi_1\rangle \otimes |\psi_1\rangle + |\psi_2\rangle \otimes |\psi_2\rangle$$

Whereas

$$\begin{aligned} U(|\psi_1\rangle \otimes |0\rangle + |\psi_2\rangle \otimes |0\rangle) &= U((|\psi_1\rangle + |\psi_2\rangle) \otimes |0\rangle) \\ &= (|\psi_1\rangle + |\psi_2\rangle) \otimes (|\psi_1\rangle + |\psi_2\rangle) \\ &\neq |\psi_1\rangle \otimes |\psi_1\rangle + |\psi_2\rangle \otimes |\psi_2\rangle \end{aligned}$$

□

Remark. *More generally, for any vector space V, the following map cannot be linear:*

$$\begin{aligned} f : V &\longrightarrow V \otimes V \\ x &\longmapsto x \otimes x \end{aligned}$$

Remark. *Sometimes CNOT is called COPY for the following reason, but this does not contradict the no-cloning theorem.*

$$\begin{aligned} CNOT : \mathbb{C}^2 \otimes \mathbb{C}^2 &\longrightarrow \mathbb{C}^2 \otimes \mathbb{C}^2 \\ |0\rangle \otimes |0\rangle &\longmapsto |0\rangle \otimes |0\rangle \\ |0\rangle \otimes |1\rangle &\longmapsto |0\rangle \otimes |1\rangle \\ |1\rangle \otimes |0\rangle &\longmapsto |1\rangle \otimes |1\rangle \\ |1\rangle \otimes |1\rangle &\longmapsto |1\rangle \otimes |0\rangle \end{aligned}$$

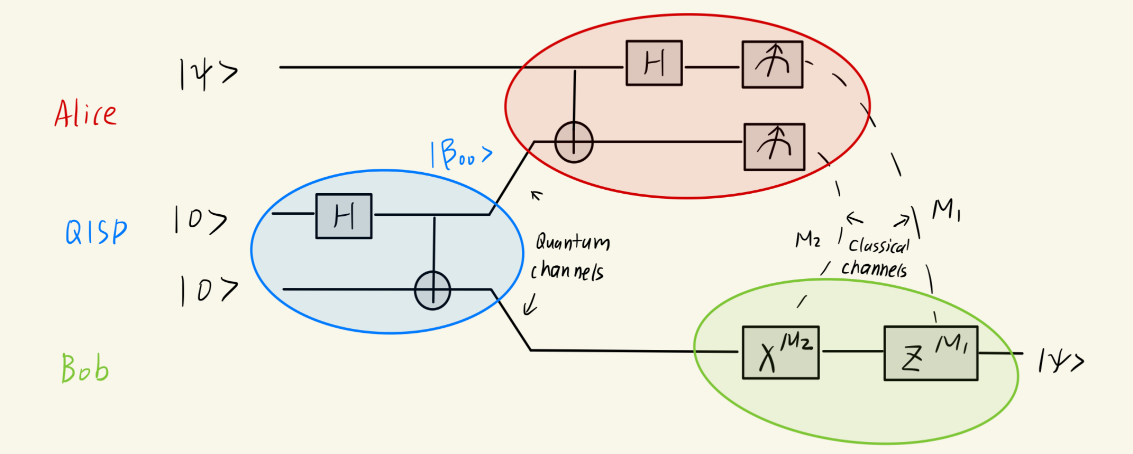
Typically, we treat the first qubit as the control and the second qubit as the input. However, if we take the first one as the input and the second one as the ancilla, then CNOT copies the input to the ancilla if ancilla=$|0\rangle$, flips and copies the input to the ancilla if ancilla=$|1\rangle$. The name COPY is okay if we remember it's only copying with respect to the computational basis. Notice that CNOT does not copy an arbitrary qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ since

$$CNOT((\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle) = CNOT(\alpha|00\rangle + \beta|10\rangle) = \alpha|00\rangle + \beta|11\rangle \neq (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

($|00\rangle$ is just another notation for $|0\rangle \otimes |0\rangle$.)

2 Superdense Coding

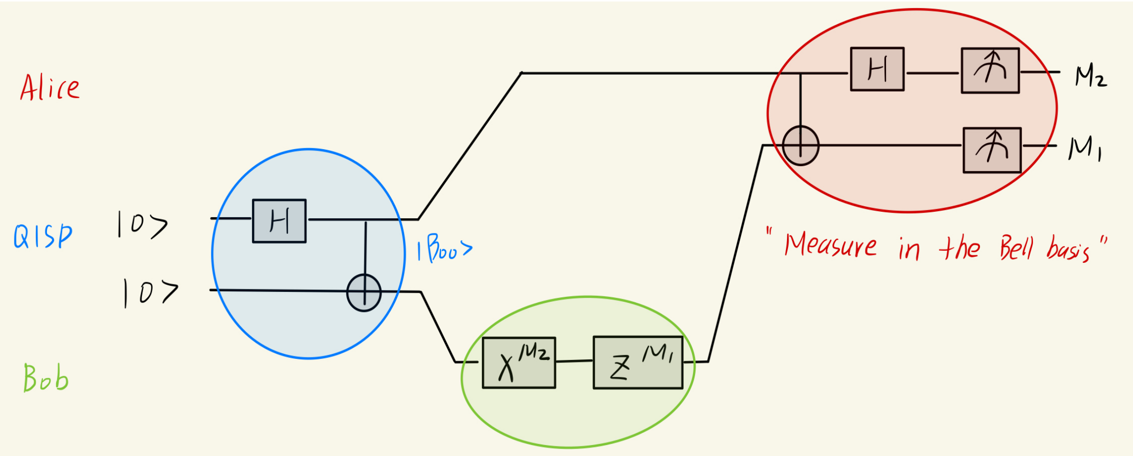
Recall the teleportation circuit:



where the Bell states are (upto a rescaling constant $\frac{1}{\sqrt{2}}$)

$$
\begin{aligned}
|\beta_{00}\rangle &= |00\rangle + |11\rangle \\
|\beta_{01}\rangle &= |01\rangle + |10\rangle \\
|\beta_{10}\rangle &= |00\rangle - |11\rangle \\
|\beta_{11}\rangle &= |01\rangle - |10\rangle
\end{aligned}
$$

Superdense coding is a way to “reverse” quantum teleportation so Bob can send two classical bits to Alice using only one qubit (assuming Alice and Bob always share a Bell pair).



Suppose Bob wants to send a messages M_2M_1, let C be the above circuit, then we claim that $C|00\rangle = |M_2M_1\rangle$. Indeed, if we let

$$|\psi\rangle := (Id \otimes Z^{M_1}X^{M_2})|\beta_{00}\rangle$$

then casework gives us the following table

M_2M_1	$\|\psi\rangle$
00	$\|\beta_{00}\rangle$
01	$\|\beta_{01}\rangle$
10	$\|\beta_{10}\rangle$
11	$\|\beta_{11}\rangle$

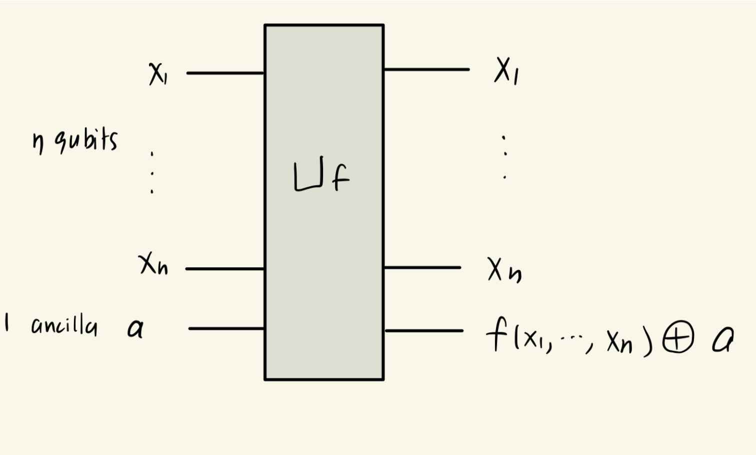
Note that Alice is applying the reverse of the circuit that the QISP implements, which takes the Bell basis back to the computational basis. Thus, when she measures, she gets the message M_2M_1, as claimed.

Remark. *Holevo's theorem implies a quantum channel that can reliably encode n qubits cannot reliably encode more than n bits.*

3 Bernstein-Vazirani Algorithm

3.1 Phase Kickback

Suppose $f : \{0,1\}^n \longrightarrow \{0,1\}$ is a Boolean function. As usual, let U_f be the unitary dilation of f, which acts on n input qubits and 1 ancilla qubit in the computational basis as $U_f|x,a\rangle = |x, f(x) \oplus a\rangle$. As a circuit, we write this



Instead of encoding the value $f(x_1, \ldots, x_n)$ in an ancilla register, we could alternatively encode it in a *phase* on $|x_1, \ldots, x_n\rangle$. Indeed, consider the following unitary

$$\begin{aligned} R_f : (\mathbb{C}^2)^{\otimes n} &\longrightarrow (\mathbb{C}^2)^{\otimes n} \\ |x\rangle &\longmapsto (-1)^{f(x)}|x\rangle \end{aligned}$$

which is diagonal in computational basis.

Claim: Oracle access to U_f is equivalent to oracle access to R_f. (Going from U_f to R_f is easy; we will discuss the other direction later after going over phase estimation.)

3.2 Algorithm

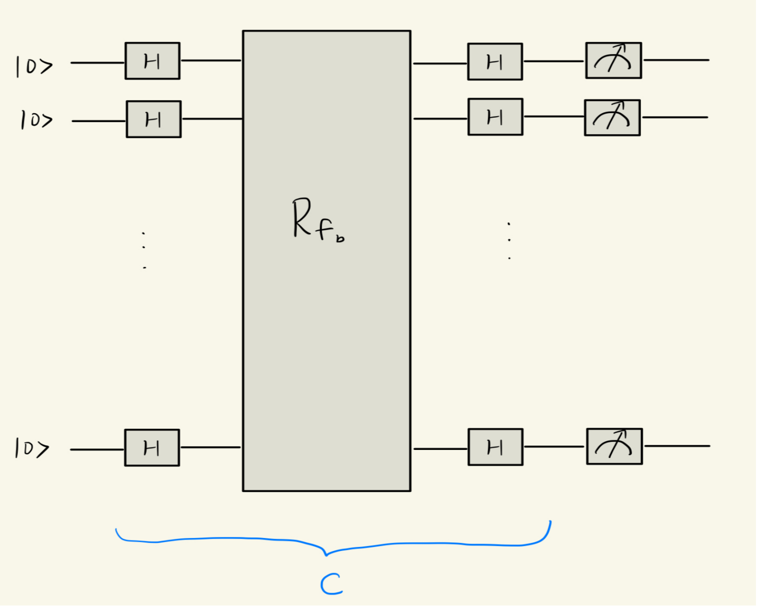
The Bernstein-Vazirani problem "hides" a bit string inside of a phase oracle that implements the dot product with the hidden bit string, and asks us to find the hidden bit string.

More precisely, we have a bitstring b of length n hidden by a function f_b:

$$\begin{aligned} f_b : \{0,1\}^n = (\mathbb{Z}/2\mathbb{Z})^n &\longrightarrow \mathbb{Z}/2\mathbb{Z} = \{0,1\} \\ x &\longmapsto x \cdot b := x_1b_1 + \ldots x_nb_n \end{aligned}$$

Given black-box access to f_b, we want to find b. Classically, even with a probabilistic algorithm, we need at least n calls to the oracle to determine b. On the other hand, given quantum oracle access to f_b via construction R_{f_b}, we need only 1 call to determine b with probability 1.

Claim: In the following diagram, the bitstring we measure is always b (i.e. with probability 1). In other words, $C|0\ldots0\rangle = |b\rangle$.



To prove this, we will need the following lemma. (You will prove this lemma in Homework 4, Problem 2).

Lemma 2. *Let H be the Hadamard matrix, then*

$$H^{\otimes n}|x\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} (-1)^{x\cdot y}|y\rangle$$

In particular

$$H^{\otimes n}|0\ldots0\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} |y\rangle$$

Now we prove the claim.

Proof. By definition of C, definition of R_{f_b}, the fact that $b+y=b-y$ in $\mathbb{Z}/2\mathbb{Z}$, and the lemma above,

$$\begin{aligned}
C|0\dots 0\rangle &= H^{\otimes n}R_{f_b}H^{\otimes n}|0\dots 0\rangle \\
&= H^{\otimes n}R_{f_b}(\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle) \\
&= H^{\otimes n}(\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}R_{f_b}|x\rangle) \\
&= H^{\otimes n}(\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}(-1)^{b\cdot x}|x\rangle) \\
&= \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}(-1)^{b\cdot x}H^{\otimes n}|x\rangle \\
&= \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}(-1)^{b\cdot x}(\frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}|y\rangle) \\
&= \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{x\cdot(b+y)}|y\rangle \\
&= \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{x\cdot(b-y)}|y\rangle \\
&= \frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{x\cdot(b-b)}|b\rangle \qquad (1) \\
&= \frac{1}{2^n}|b\rangle \qquad \text{(or just } |b\rangle\text{)}
\end{aligned}$$

In (1), we used the fact that for $y \neq b$, the terms $(-1)^{x\cdot(b-y)}$ cancel out by symmetry, i.e., $\sum_{y\neq b}(-1)^{x\cdot(b-y)} = 0$. □

4 BQP ⊂ PSPACE

Lemma 3. *Given a quantum circuit C on n qubits over a fixed finite gate set $\mathscr{G}$, an $\varepsilon > 0$, and two bitstrings $x,y \in \{0,1\}^n$, there exists a classical algorithm to find a complex number z such that $|z - \langle y|C|x\rangle| < \varepsilon$ in polynomial time as a function of the size of C.*

Proof.

$$\begin{aligned}
C &= g_l \circ g_{l-1} \circ \cdots \circ g_1 && (g_i \in \mathscr{G}) \\
&= g_l \circ id \circ g_{l-1} \circ id \circ \cdots \circ id \circ g_1 \\
&= \sum_{s_1,\dots,s_{l-1}=0}^{2^n-1} g_l|s_{l-1}\rangle\langle s_{l-1}|g_{l-1}|s_{l-2}\rangle\dots\langle s_1|g_1 && (id = \sum_{s=0}^{2^n-1}|s\rangle\langle s| \text{ by the spectral decomposition}) \\
\langle y|C|x\rangle &= \sum_{s_1,\dots,s_{l-1}=0}^{2^n-1}\langle y|g_l|s_{l-1}\rangle\langle s_{l-1}|g_{l-1}|s_{l-2}\rangle\dots\langle s_1|g_1|x\rangle
\end{aligned}$$

We assume we know the entries of any gate in $\mathscr{G}$ "exactly." Each term in the last expression is exactly such an entry. Now compute $\langle y|C|x\rangle$ using a "running total" iteratively / dynamically. This takes exponential time (because there are exponentially many terms), but so long as we just got "one by one" then PSPACE is sufficient. □

With more work (in particular, if we keep track of the dependence of the previous procedure by letting $\varepsilon = \frac{1}{2^n}$, then we can show

Theorem 4. *BQP* $\subset$ *PSPACE*