ACCQ206

Lecturer: Alex B. Grilo
Lecture # 03 - Entanglement + algorithms

Throughout this exercise list, we call $|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Entanglement

1. One particular useful application of quantum teleportation is *entanglement swapping*. Suppose that Alice and Bob share an EPR pair, and Bob and Charlie share a second EPR pair (see Figure 1). Show that via quantum teleportation, Bob can help Alice and Charlie share an EPR pair with classical communication only. Does Bob share an EPR pair with any other party after the execution of this protocol?
   Solution: The three parties share the state

$$
\begin{aligned}
&\frac{1}{2}(|00\rangle_{AB} + |11\rangle_{AB})(|00\rangle_{B'C} + |11\rangle_{B'C}) \\
&= \frac{1}{2}(|0000\rangle_{ABB'C} + |0011\rangle_{ABB'C}|1100\rangle_{ABB'C} + |1111\rangle_{ABB'C}) \\
&= \frac{1}{2}(|0000\rangle_{BB'AC} + |0101\rangle_{BB'AC}|1010\rangle_{BB'AC} + |1111\rangle_{BB'AC}) \\
&= \frac{1}{2\sqrt{2}}\Big((|\Psi_{00}\rangle_{BB'} + |\Psi_{01}\rangle_{BB'})|00\rangle_{AC} + (|\Psi_{10}\rangle_{BB'} + |\Psi_{11}\rangle_{BB'})|01\rangle_{AC} \\
&\qquad + (|\Psi_{10}\rangle_{BB'} - |\Psi_{11}\rangle_{BB'})|10\rangle_{AC} + (|\Psi_{00}\rangle_{BB'} - |\Psi_{01}\rangle_{BB'})|11\rangle_{AC}\Big) \\
&= \frac{1}{2\sqrt{2}}\Big(|\Psi_{00}\rangle_{BB'}(|00\rangle_{AC} + |11\rangle_{AC}) + |\Psi_{01}\rangle_{BB'}(|00\rangle_{AC} - |11\rangle_{AC}) \\
&\qquad + |\Psi_{10}\rangle_{BB'}(|01\rangle_{AC} + |10\rangle_{AC}) + |\Psi_{11}\rangle_{BB'}(|01\rangle_{AC} - |10\rangle_{AC})\Big) \\
&= \frac{1}{2}\sum_{a,b\in\{0,1\}} |\Psi_{ab}\rangle(X^aZ^b \otimes I)|EPR\rangle.
\end{aligned}
$$

   Bob can measure his both qubits in the Bell basis, and tell the outcome a, b to Alice. Alice then applies the Pauli correction based on these values and then Alice and Charlie share an EPR pair.

   After this protocol is run, Bob does not share any EPR pair with either party.

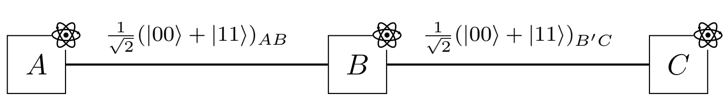


Figure 1: Setup for entanglement swapping

Density matrices

In the following exercise, we denote $((p_1, |\psi_1\rangle), (p_2, |\psi_2\rangle), ..., (p_n, |\psi_n\rangle))$ as the ensemble where we create the state $|\psi_i\rangle$ with probability p_i.

2. Compute the density matrices of:

   (a) $((1, |\psi\rangle))$ and $((1, e^{i\theta}|\psi\rangle))$.
   Solution: The density matrix of $|\psi\rangle$ is $|\psi\rangle\langle\psi|$.
   The density matrix of $e^{i\theta}|\psi\rangle$ is $e^{i\theta}e^{-i\theta}|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi|$.

   (b) $((\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle))$ and $((\frac{1}{2}, |+\rangle), (\frac{1}{2}, |-\rangle))$.
   Solution: The density matrix of $((\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle))$ is

$$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = I$$

   The density matrix of $((\frac{1}{2}, |+\rangle), (\frac{1}{2}, |-\rangle))$ is

$$\frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} + \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = I$$

   What can you conclude from the previous results?
   Solution: Different ensembles result in the same density matrix.

   Global phases do not change the density matrix $\Rightarrow$ global phases do not matter.

3. Let $|\psi\rangle_{AB} = \frac{1}{\sqrt{3}}(|1\rangle_A|00\rangle_B + |1\rangle_A|10\rangle_B + |1\rangle_A|01\rangle_B)$. Compute $Tr_A(|\psi\rangle\langle\psi|_{AB})$.
   Solution:

$$\begin{aligned}
&Tr_A(|\psi\rangle\langle\psi|_{AB}) \\
&= \frac{1}{3}Tr_A\Big(|1\rangle\langle 1|_A \otimes |00\rangle\langle 00|_B + |1\rangle\langle 1|_A \otimes |00\rangle\langle 01|_B + |1\rangle\langle 1|_A \otimes |00\rangle\langle 10|_B \\
&\qquad + |1\rangle\langle 1|_A \otimes |01\rangle\langle 01|_B + |1\rangle\langle 1|_A \otimes |01\rangle\langle 00|_B + |1\rangle\langle 1|_A \otimes |01\rangle\langle 10|_B \\
&\qquad + |1\rangle\langle 1|_A \otimes |10\rangle\langle 10|_B + |1\rangle\langle 1|_A \otimes |10\rangle\langle 00|_B + |1\rangle\langle 1|_A \otimes |10\rangle\langle 01|_B\Big) \\
&= \frac{1}{3}\Big(Tr_A(|1\rangle\langle 1|_A \otimes |00\rangle\langle 00|_B) + Tr_A(|1\rangle\langle 1|_A \otimes |00\rangle\langle 01|_B) + Tr_A(|1\rangle\langle 1|_A \otimes |00\rangle\langle 10|_B) \\
&\qquad + Tr_A(|1\rangle\langle 1|_A \otimes |01\rangle\langle 01|_B) + Tr_A(|1\rangle\langle 1|_A \otimes |01\rangle\langle 00|_B) + Tr_A(|1\rangle\langle 1|_A \otimes |01\rangle\langle 10|_B) \\
&\qquad + Tr_A(|1\rangle\langle 1|_A \otimes |10\rangle\langle 10|_B) + Tr_A(|1\rangle\langle 1|_A \otimes |10\rangle\langle 00|_B) + Tr_A(|1\rangle\langle 1|_A \otimes |10\rangle\langle 01|_B)\Big) \\
&= \frac{1}{3}\Big(\ \langle 1|\,1\rangle\ |00\rangle\langle 00|_B + +\ \langle 1|\,1\rangle\ |00\rangle\langle 01|_B +\ \langle 1|\,1\rangle\ |00\rangle\langle 10|_B \\
&\qquad +\ \langle 1|\,1\rangle\ |01\rangle\langle 01|_B +\ \langle 1|\,1\rangle\ |01\rangle\langle 00|_B +\ \langle 1|\,1\rangle\ |01\rangle\langle 10|_B \\
&\qquad +\ \langle 1|\,1\rangle\ |10\rangle\langle 10|_B +\ \langle 1|\,1\rangle\ |10\rangle\langle 00|_B +\ \langle 1|\,1\rangle\ |10\rangle\langle 01|_B\Big) \\
&= \frac{1}{3}\Big(|00\rangle\langle 00|_B + |00\rangle\langle 01|_B + |00\rangle\langle 10|_B + |01\rangle\langle 01|_B + |01\rangle\langle 00|_B + |01\rangle\langle 10|_B \\
&\qquad + |10\rangle\langle 10|_B + |10\rangle\langle 00|_B + |10\rangle\langle 01|_B\Big) \\
&= \left(\frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |10\rangle)\right)\left(\frac{1}{\sqrt{3}}(\langle 00| + \langle 01| + \langle 10|)\right)
\end{aligned}$$

4. Let $|W_3\rangle_{AB} = \frac{1}{\sqrt{3}}(|1\rangle_A|00\rangle_B + |0\rangle_A|10\rangle_B + |0\rangle_A|01\rangle_B)$. Compute $Tr_A(|W_3\rangle\langle W_3|_{AB})$.
Solution:

$$
\begin{aligned}
&Tr_A(|\psi\rangle\langle\psi|_{AB}) \\
&= \frac{1}{3} Tr_A\Big(|1\rangle\langle 1|_A \otimes |00\rangle\langle 00|_B + |1\rangle\langle 0|_A \otimes |00\rangle\langle 01|_B + |1\rangle\langle 0|_A \otimes |00\rangle\langle 10|_B \\
&\qquad + |0\rangle\langle 0|_A \otimes |01\rangle\langle 01|_B + |0\rangle\langle 1|_A \otimes |01\rangle\langle 00|_B + |0\rangle\langle 0|_A \otimes |01\rangle\langle 10|_B \\
&\qquad + |0\rangle\langle 0|_A \otimes |10\rangle\langle 10|_B + |0\rangle\langle 1|_A \otimes |10\rangle\langle 00|_B + |0\rangle\langle 0|_A \otimes |10\rangle\langle 01|_B \Big) \\
&= \frac{1}{3}\Big(Tr_A(|1\rangle\langle 1|_A \otimes |00\rangle\langle 00|_B) + Tr_A(|1\rangle\langle 0|_A \otimes |00\rangle\langle 01|_B) + Tr_A(|1\rangle\langle 0|_A \otimes |00\rangle\langle 10|_B) \\
&\qquad + Tr_A(|0\rangle\langle 0|_A \otimes |01\rangle\langle 01|_B) + Tr_A(|0\rangle\langle 1|_A \otimes |01\rangle\langle 00|_B) + Tr_A(|0\rangle\langle 0|_A \otimes |01\rangle\langle 10|_B) \\
&\qquad + Tr_A(|0\rangle\langle 0|_A \otimes |10\rangle\langle 10|_B) + Tr_A(|0\rangle\langle 1|_A \otimes |10\rangle\langle 00|_B) + Tr_A(|0\rangle\langle 0|_A \otimes |10\rangle\langle 01|_B) \Big) \\
&= \frac{1}{3}\Big(\langle 1|\,1\rangle\,|00\rangle\langle 00|_B + + \langle 1|\,0\rangle\,|00\rangle\langle 01|_B + \langle 1|\,0\rangle\,|00\rangle\langle 10|_B \\
&\qquad + \langle 0|\,0\rangle\,|01\rangle\langle 01|_B + \langle 0|\,1\rangle\,|01\rangle\langle 00|_B + \langle 0|\,0\rangle\,|01\rangle\langle 10|_B \\
&\qquad + \langle 0|\,0\rangle\,|10\rangle\langle 10|_B + \langle 0|\,1\rangle\,|10\rangle\langle 00|_B + \langle 0|\,0\rangle\,|10\rangle\langle 01|_B \Big) \\
&= \frac{1}{3}\Big(|00\rangle\langle 00|_B + |01\rangle\langle 01|_B + |01\rangle\langle 10|_B + |10\rangle\langle 10|_B + |10\rangle\langle 01|_B \Big) \\
&= \frac{1}{3}|00\rangle\langle 00| + \frac{2}{3}\left(\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)\right)\left(\frac{1}{\sqrt{2}}(\langle 01| + \langle 10|)\right)
\end{aligned}
$$

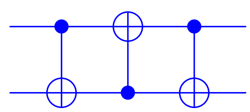
Quantum circuits

5. Show that you can use the CCNOT gate to compute the NAND gate. Since NAND is universal for classical computation, this means that every problem that can be solved with classical circuits can be also solved by quantum circuits.
Solution: $CCNOT|a\rangle|b\rangle|1\rangle = |a\rangle|b\rangle|1\oplus ab\rangle = |a\rangle|b\rangle|NOT(ab)\rangle = |a\rangle|b\rangle|NOT(AND(a,b))\rangle$

6. The SWAP gate works as $SWAP|a\rangle|b\rangle = |b\rangle|a\rangle$.

   (a) Show that SWAP gate is unitary.
   Solution: The matrix for SWAP is $\begin{pmatrix} 1&0&0&0 \\ 0&0&1&0 \\ 0&1&0&0 \\ 0&0&0&1 \end{pmatrix}$.
   We have that $SWAP^\dagger = SWAP$ and $SWAP \cdot SWAP^\dagger = SWAP^2 = I$.

   (b) Show how to implement the SWAP gate with three CNOT gates.
   Solution:



$$CNOT_{1,2}CNOT_{2,1}CNOT_{1,2}|a,b\rangle = CNOT_{1,2}CNOT_{2,1}|a, b\oplus a\rangle$$
$$= CNOT_{1,2}|a\oplus b\oplus a, b\oplus a\rangle - CNOT_{1,2}|b, b\oplus a\rangle = |b, b\oplus a\oplus b\rangle = |b,a\rangle.$$

7. Consider the circuit in Figure 2.

   (a) Compute the output of the quantum circuit if the input is $|b\rangle|a\rangle$, for $a, b \in \{0,1\}$.
   Solution:

   $$CNOT_{1,2}H_1|b\rangle|a\rangle = CNOT(H\otimes I)|b\rangle|a\rangle = \frac{1}{\sqrt{2}}CNOT(|0\rangle + (-1)^b|1\rangle)|a\rangle$$
   $$= \frac{1}{\sqrt{2}}(|0\rangle|a\rangle + (-1)^b|1\rangle|1\oplus a\rangle) = |\Psi_{ab}\rangle.$$

   (b) Write the 4×4 matrix that describes that circuit.
   Solution:

   $$CNOT_{1,2}H_1 = CNOT(H\otimes I) = \begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\left(\frac{1}{\sqrt{2}}\begin{pmatrix} I & I\\ I & -I\end{pmatrix}\right)$$
   $$= \frac{1}{\sqrt{2}}\begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix} 1&0&1&0\\0&1&0&1\\1&0&-1&0\\0&1&0&-1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1&0&1&0\\0&1&0&1\\0&1&0&-1\\1&0&-1&0\end{pmatrix}$$

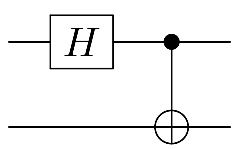
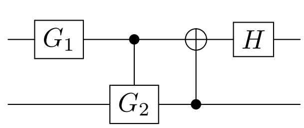
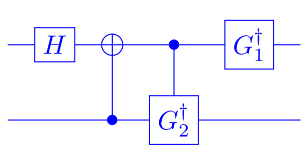


Figure 2: Circuit for Exercise 7

8. Write the circuit corresponding to the inverse of (where G_1 and G_2 are arbitrary 1-qubit gates)



Solution:



Quantum algorithms

We say that $f : \{0,1\}^n \to \{0,1\}$ is a linear function if there exists some value $s \in \{0,1\}^n$ such that it can be written as $f(x) = x \cdot s \pmod 2$.

9. Suppose that you have (classical) oracle access to a linear function $f_s(x) = s \cdot x \pmod 2$. Show a classical algorithm that learn s with n queries.
   Solution: For the i-th query, set the i-th bit of x to be 1 and all other bits to 0. This query answers s_i. After n queries, we learn each qubit of s.

10. Suppose now that you have quantum oracle access to f_s (i.e. you have access to the unitary $O_{f_s}|x\rangle|b\rangle = |x\rangle|b \oplus f_s(x)\rangle$). The Bernstein-Vazirani algorithm (Figure 3) allows us to find s with a single quantum query to this oracle.

    (a) What is the state of the algorithm after the first layer of Hadamard gates?
    Solution: $H^{\otimes(n+1)}|0\rangle^{\otimes n}|1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|-\rangle$

    (b) What is the state of the algorithm after the query to the oracle?
    Solution: $\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot s}|x\rangle|-\rangle$

    (c) What is the state of the algorithm after the last layer of Hadamards?
    Solution:

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

    The amplitude of $y = s$ is

    $$\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot s\oplus x\cdot s} = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{2(x\cdot s)} = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} 1 = 1.$$

    The amplitude of any $y^* \neq s$ is

    $$\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot s\oplus x\cdot y^*} = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot(y^*\oplus s)} = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot z},$$

    where $z = y^* \oplus s \neq 0^n$. Since $z \neq 0^n$, half of the values of x have $x \cdot z = 0 \pmod 2$ and half of the values of x have $x \cdot z = 1 \pmod 2$, and therefore the amplitude of y^* is 0.

    (d) Compute the probability of measuring s on the first register.
    Solution: The measurement outcome is s with probability 1.

11. Compute every step of the computation of the Bernstein-Vazirani algorithm with oracle access to the linear function $f(x_1, x_2) = x_1 + x_2$. What is the value of s?
    Solution: After the first layer of Hadamards:

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

    After the oracle query:

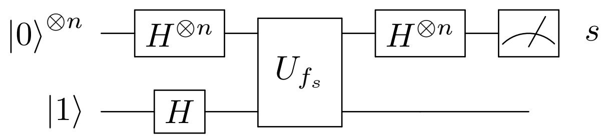


Figure 3: Bernstein-Vazirani algorithm

$\frac{1}{2}(|00\rangle|-\rangle - |01\rangle|-\rangle - |01\rangle|-\rangle + |11\rangle|-\rangle)$
After the second layer of Hadamards
$|11\rangle$

We have that the value of s is 11.