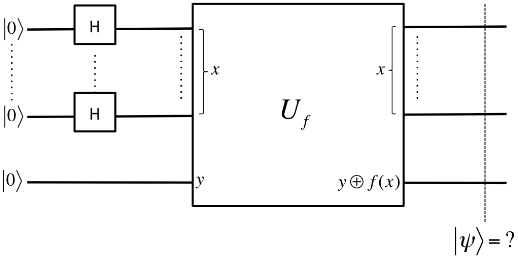
COL866: Quantum Computation and Information

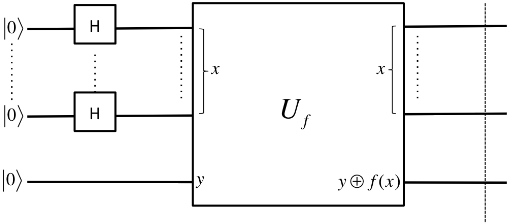
Ragesh Jaiswal, CSE, IIT Delhi

Introduction

- Question: Can we generalize this idea for boolean functions over multiple bit inputs?
- Consider any boolean function over n-bit inputs $f : \{0,1\}^n \rightarrow \{0,1\}$.
- What is the output of the following circuit?

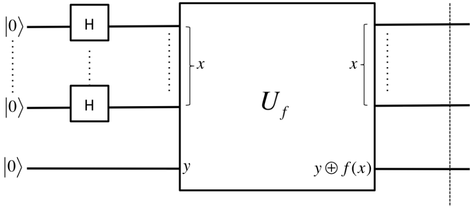


- Question: Can we generalize this idea for boolean functions over multiple bit inputs?
- Consider any boolean function over n-bit inputs $f : \{0,1\}^n \rightarrow \{0,1\}$.
- What is the output of the following circuit?



$$|\psi\rangle = \frac{1}{2^{n/2}} \sum_x |x\rangle |f(x)\rangle$$

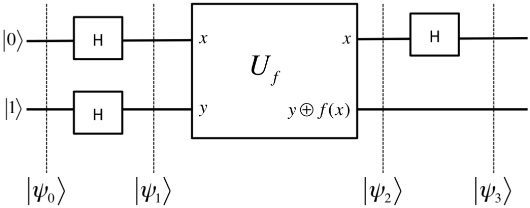
- Question: Can we generalize this idea for boolean functions over multiple bit inputs?
- Consider any boolean function over n-bit inputs $f : \{0,1\}^n \rightarrow \{0,1\}$.
- What is the output of the following circuit?



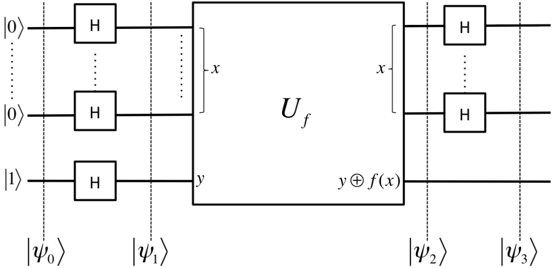
$$|\psi\rangle = \frac{1}{2^{n/2}} \sum_x |x\rangle |f(x)\rangle$$

- Even though final state encodes evaluation of the function on all inputs, what we can measure is only one of them. So, it is important that we do not get carried away by the potential quantum parallelism exhibited in the above circuit.

- Even though final state encodes evaluation of the function on all inputs, what we can measure is only one of them. So, it is important that we do not get carried away by the potential quantum parallelism exhibited in the above circuit.
- Exploiting the parallelism in more realistic way is the key challenge while designing quantum algorithms.
- Consider the case of a boolean function on single-bit inputs $f : \{0,1\} \rightarrow \{0,1\}$. Suppose we would want to know if $f(0) = f(1)$. Here is a quantum circuit that solves this.

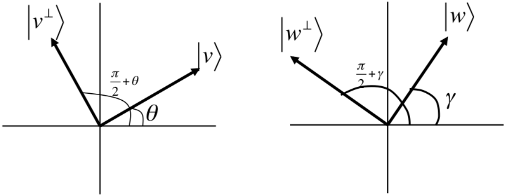


- The previous problem was a specific case of the more general Deutsch's problem that further demonstrates the power of quantum algorithms.
- Deutsch's problem: Bob has a function $f : \{0,1\}^n \rightarrow \{0,1\}$ that is either a constant function or a balanced function (i.e., f is 0 on $2^n/2$ inputs). Alice wants to determine what kind of function Bob has but can make a query to the function only once.
- The following circuit does this:



Introduction: Entanglement

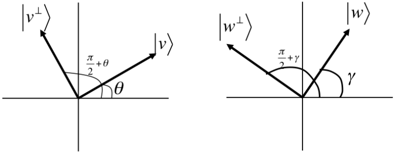
- We said that one can measure in any orthonormal basis.
- Often, we would want to measure in a basis that is rotation of the standard basis.



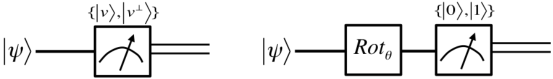
- So, $|v\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$ and $|v^{\perp}\rangle = -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle$
- Claim: Making a measurement in the $\{|v\rangle, |v^{\perp}\rangle\}$ basis is the same as making a measurement in the standard basis after applying the following gate:

$$Rot_{\theta} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$$

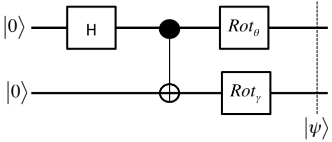
- We said that one can measure in any orthonormal basis.
- Often, we would want to measure in a basis that is rotation of the standard basis.



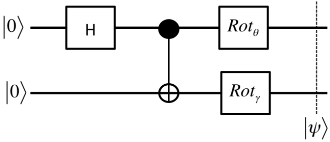
- So, $|v\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$ and $|v^{\perp}\rangle = -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle$
- Claim: Making a measurement in the $\{|v\rangle, |v^{\perp}\rangle\}$ basis is the same as making a measurement in the standard basis after applying the following gate: $Rot_\theta = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$.
- In terms of circuits, the following two circuits exhibit the same measurement results.



- Let $\Delta = \theta - \gamma$. What is output of the following circuit $|\psi\rangle$?



- Let $\Delta = \theta - \gamma$. What is output of the following circuit $|\psi\rangle$?

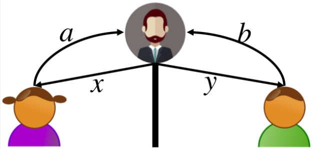


$|\psi\rangle = \frac{1}{\sqrt{2}} (\cos\Delta\,|00\rangle + \sin\Delta\,|01\rangle - \sin\Delta\,|10\rangle + \cos\Delta\,|11\rangle)$

- Corollary: Suppose Alice has the first qubit and Bob has the second qubit. Then on measurement of $|\psi\rangle$, the output is same with probability $\cos^2\Delta$ and different with probabiity $\sin^2\Delta$.

CHSH game

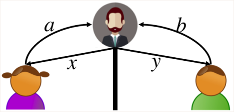
Alice and Bob receive randomly generated bits $x, y \in \{0, 1\}$ respectively from a Charlie. Their goal is to respond with bits a and b such that $a \oplus b = x \wedge y$. They are not allowed to communicate after receiving x and y.



- Lemma 1: There is no classical deterministic or randomized strategy that allows Alice and Bob to win with probability more than $3/4$.
- Lemma 2: There is a quantum strategy that allows Alice and Bob to win with probability $\cos^2 \pi/8 \approx 0.85 > 3/4$.

CHSH game

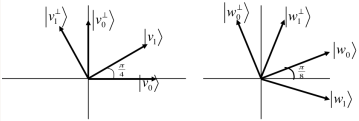
Alice and Bob receive randomly generated bits $x, y \in \{0, 1\}$ respectively from a Charlie. Their goal is to respond with bits a and b such that $a \oplus b = x \wedge y$. They are not allowed to communicate after receiving x and y.



- Lemma 2: There is a quantum strategy that allows Alice and Bob to win with probability $\cos^2 \pi/8 \approx 0.85 > 3/4$.

Quantum strategy

- Alice and Bob share an EPR pair $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$ to start with.
- Alice and Bob measure in basis $\{|v_x\rangle, |v_x^{\perp}\rangle\}$, $\{|w_x\rangle, |w_x^{\perp}\rangle\}$ respectively and they simply return their measurement outputs.



End