CS621/CSL611
Quantum Computing For Computer Scientists

Quantum Circuits and Protocols

Dhiman Saha

Winter 2024

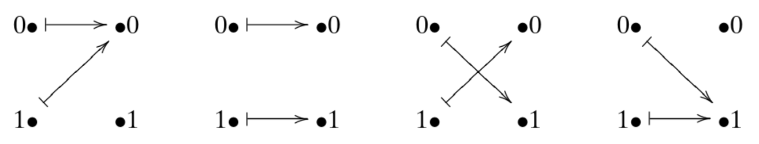
IIT Bhilai

Deutsch's Algorithm

Deutsch's Problem: Balanced or Constant

Deutsch's Problem

- Set of functions from $f : \{0, 1\} \to \{0, 1\}$

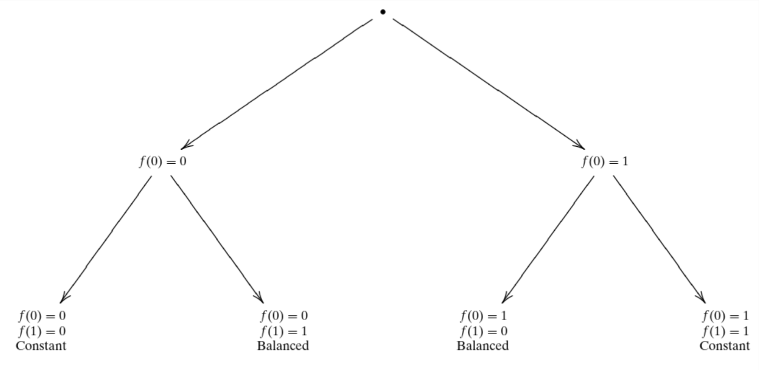


- f is balanced if $f(0) \neq f(1)$
- f is constant if $f(0) = f(1)$

Problem Definition

Given a function $f : \{0, 1\} \to \{0, 1\}$ as a **black-box**, where one can evaluate an input, but **cannot** *look inside* and *see* how the function is defined, determine if the function is **balanced** or **constant**.

- Evaluate f on both inputs. Compare the outputs.
- With a classical computer, f **must** be evaluated **twice**.



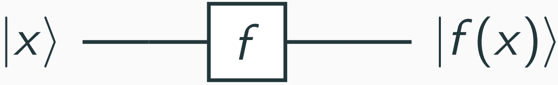
- Can we do better (one evaluation only) with a quantum computer?

Superposition and Quantum Interference

- A quantum computer can be in a superposition of two basic states at the same time.
- **Deutsch's algorithm** will let us put together a state that has *all of the output values of the function associated with each input value* in a superposition state.
- Then we will use **quantum interference** (QI) to find out if the given function is constant or balanced.

- **Note:** whether a function on a single bit is constant or balanced is a *global property.*
- **Recall:** QI allows to deduce certain *global properties* of the function

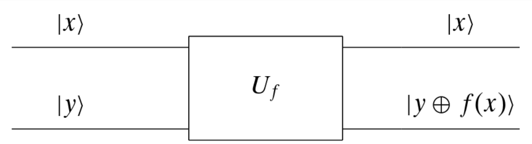
- Need to adapt the problem to fit the quantum computing model
- Function black-box **must** conform to a valid quantum operation.
- Action of the device simulating the function **must** correspond to a **unitary** transformation
- A one-qubit gate is not sufficient. Why?



- Need to adapt the problem to fit the quantum computing model
- Function black-box **must** conform to a valid quantum operation.
- Action of the device simulating the function **must** correspond to a **unitary** transformation
- A one-qubit gate is not sufficient. Why?
- Is the correspond matrix unitary? Check for $f(x) = 0$

$$|x\rangle \;\text{———}\; \boxed{f} \;\text{———}\; |f(x)\rangle$$

- For any function $f : \{0,1\} \to \{0,1\}$ a 2-qubit quantum gate U_f is defined as:



- **Note:** The matrix corresponding to U_f is unitary for any function f.
- Cross-check for the bit-flip function: $f(0) = 1$ and $f(1) = 0$

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

- For any function f, the matrix corresponding to U_f will always be a permutation matrix
- **Note:** Permutation matrices are always unitary.

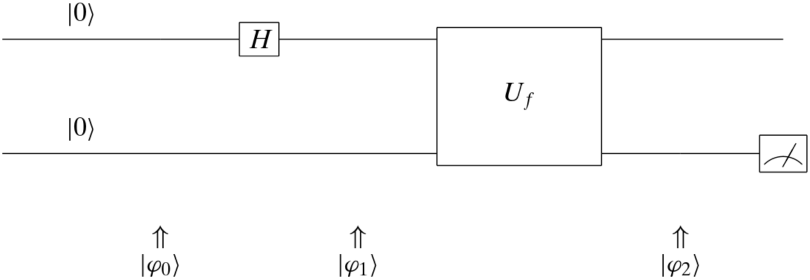
A More General Formulation

- Let $f : \{0,1\}^n \rightarrow \{0,1\}^m$ be any function for +ve integers n and m
- The associated quantum transformation U_f is given as:

$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus f(x)\right\rangle$$

- The associated matrix will always be a **permutation** matrix, and is therefore **unitary**.

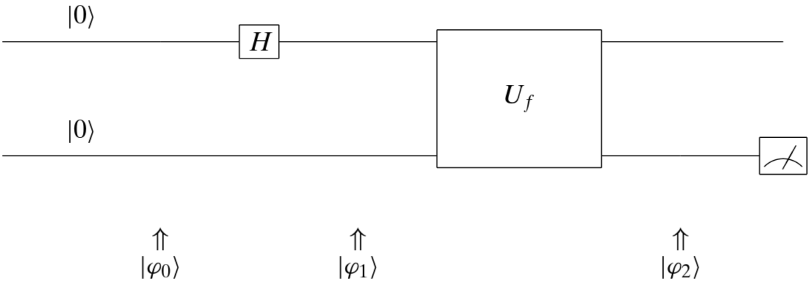
Superposition On The Top Input



- Initial State:

$$|\phi_0\rangle = |0\rangle\,|0\rangle$$

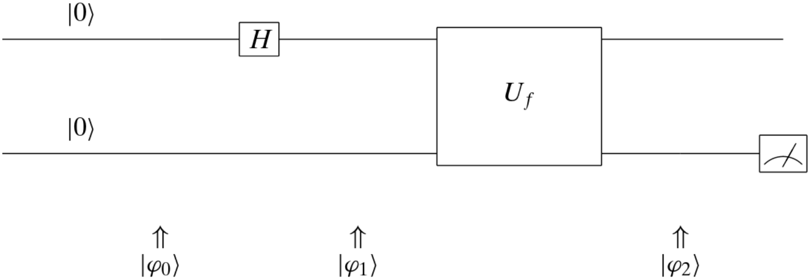
Superposition On The Top Input



- After applying Hadamard on first qubit

$$|\phi_1\rangle = H \otimes I\, |00\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}$$

Superposition On The Top Input



- After applying U_f

$$|\phi_2\rangle = U_f\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|0\rangle = \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$$

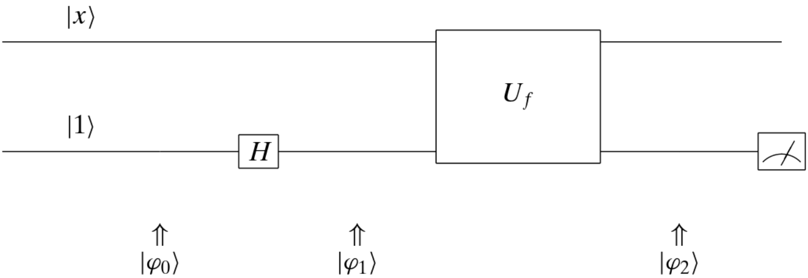
Point-to-Ponder

$$|\phi_2\rangle = \boxed{\underbrace{\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}}_{\text{Superposition state with \textbf{all} pairs of } x,\, f(x) \text{ represented}}}$$

Can this be exploited?

- **NO**. Recall how quantum measurements work
- For a simple function on bits we can learn the value of $f(0)$ or $f(1)$, but not both simultaneously
- Even though they are **simultaneously** present in the **premeasurement** state
- This is **worse** than what could be done with a classical computer. How?

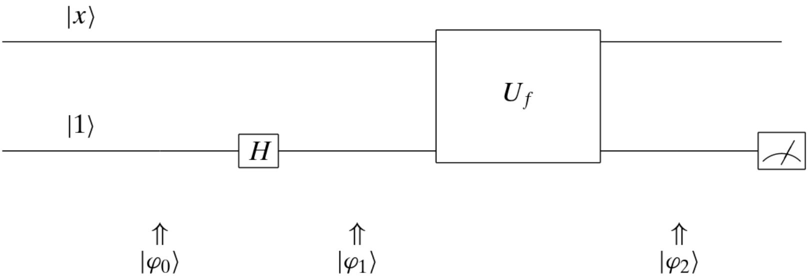
Superposition On The Bottom Input



- Initial State:

$$|\phi_0\rangle = |x\rangle\,|1\rangle$$

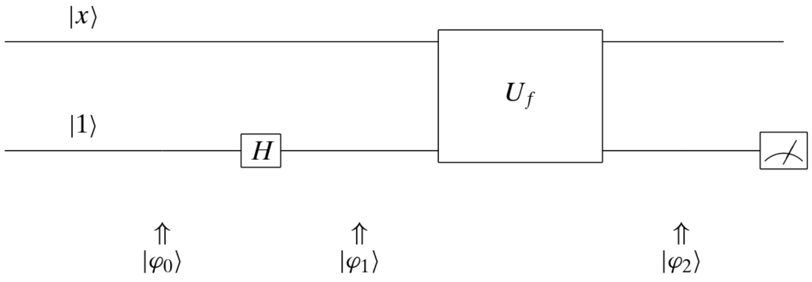
Superposition On The Bottom Input



- After applying Hadamard on second qubit

$$|\phi_1\rangle = I \otimes H\,|x1\rangle = |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \frac{|x0\rangle - |x1\rangle}{\sqrt{2}}$$

Superposition On The Bottom Input



- After applying U_f

$$|\phi_2\rangle = |x\rangle \left(\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} \right) = |x\rangle \frac{|f(x)\rangle - |\neg f(x)\rangle}{\sqrt{2}}$$

- So the final state is:

$$|\phi_2\rangle = \begin{cases} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right), & \text{if } f(x) = 0 \\ |x\rangle \left(\frac{|1\rangle - |0\rangle}{\sqrt{2}}\right), & \text{if } f(x) = 1 \end{cases}$$

- Alternatively,

Unaltered by U_f

$$|\phi_2\rangle = (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

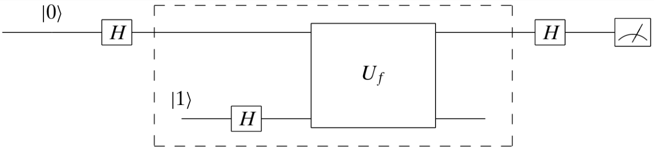
Again, can this be exploited? **Answer: No**

- The top qubit will be in state $|x\rangle$
- The bottom qubit will be either in state $|0\rangle$ or in state $|1\rangle$.

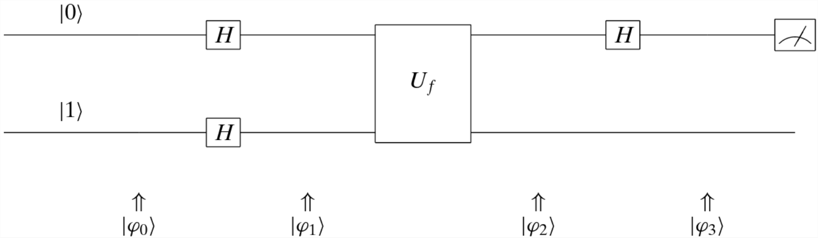
- Deutschs algorithm works by putting both the top and the bottom qubits into a superposition.[1]

Steps $|\psi_{out}\rangle = (H \otimes I)U_f(H \otimes H)|0\rangle|1\rangle$

1. Apply Hadamard gates to the input state $|0\rangle|1\rangle$ to produce a product state of two superpositions.
2. Apply U_f to that product state.
3. Apply a Hadamard gate to the first qubit only
4. Measure the first qubit



[1]Exploits the fact that the system is in a superposition state $\Sigma|x\rangle|f(x)\rangle$ to infer a global property of the function: balanced or constant

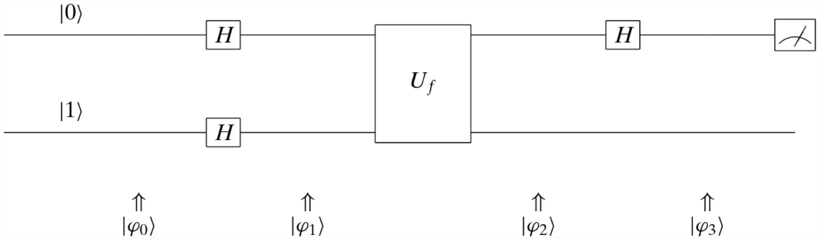


- Initial State:

$$|\phi_0\rangle = |01\rangle$$

- Applying Hadamard gates: $H \otimes H\,|01\rangle$

$$\begin{aligned}|\phi_1\rangle &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)\end{aligned}$$



- Recall $U_f(I \otimes H)|x\rangle|1\rangle = \boxed{\underbrace{(-1)^{f(x)}|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)}_{\text{From Attempt-2}}}$
- After $U_f(H \otimes H)|0\rangle|1\rangle$

$$|\phi_2\rangle = \boxed{\left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right)} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Unaltered by U_f

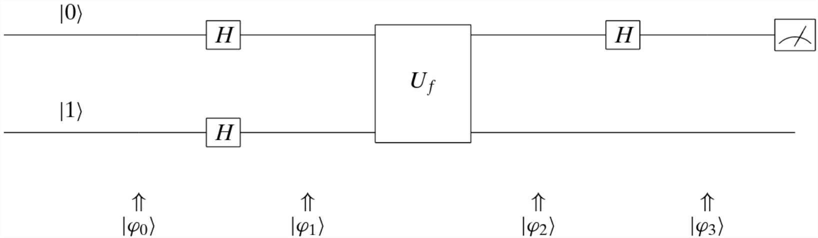
- What is the nature of $(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$ for any general function f?

$$(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle = \begin{cases} +1(|0\rangle + |1\rangle) & f \rightarrow \text{ Constant 0} \\ -1(|0\rangle + |1\rangle) & f \rightarrow \text{ Constant 1} \\ +1(|0\rangle - |1\rangle) & f \rightarrow \text{ Identity} \\ -1(|0\rangle - |1\rangle) & f \rightarrow \text{ Bit Flip} \end{cases}$$

- So $|\phi_2\rangle$ is given by:

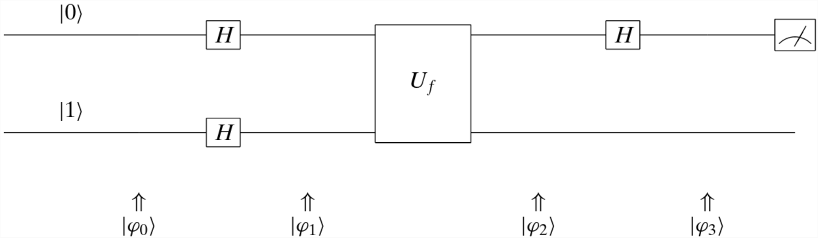
$$|\phi_2\rangle = \begin{cases} \boxed{(\pm 1)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \quad \text{if } f \rightarrow \text{ constant}} \\ \boxed{(\pm 1)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \quad \text{if } f \rightarrow \text{ balanced}} \end{cases}$$

Note: The first qubit is **differentiating** factor that can be **exploited**



- **Recall:** $H\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) = |0\rangle$ and $H\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) = |1\rangle$.
- Applying H on top qubit we get:

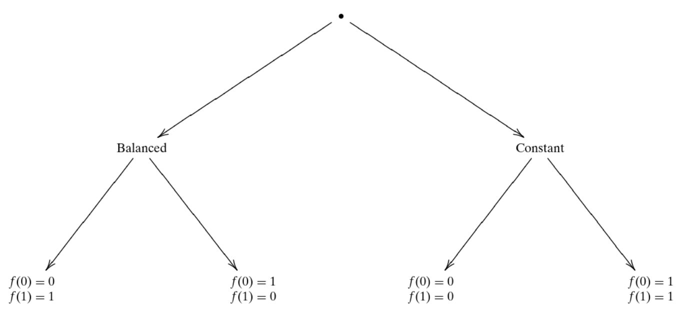
$$|\phi_3\rangle = \begin{cases} (\pm 1)|0\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if } f \rightarrow \text{ constant} \\ (\pm 1)|1\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if } f \rightarrow \text{ balanced} \end{cases}$$



- Measure the top qubit
  - If it is in state $|0\rangle$, then f is a constant function
  - If it is in state $|1\rangle$, then f is a balanced function
- Achieved with **only** one function evaluation in U_f
- The sign in $|\phi_3\rangle$ gives further info but it is **not** exploitable

Point-to-Ponder

- In this algorithm, **single-qubit interference** is applied to the first qubit allowing us to distinguish between the two cases of the output of the function
- Did we gain information that was not there? No



- The Hadamard matrices are changing the question that we are asking (**change of basis**)

Intuition behind the Deutsch algorithm

Performing a change of basis problem

- Start in the canonical basis.
- The first Hadamard matrix is used as a **change of basis** matrix to go into a *balanced superposition of basic states*.
- While in this non-canonical basis, we evaluate f with the bottom qubit in a superposition.
- The last Hadamard matrix is used as a change of basis matrix to revert back to the canonical basis.

- For every ket $|\psi\rangle$ there is a corresponding object $\langle\psi|$, called "bra". Intuition comes combining a bra and a ket together to get "braket"

Definition

For any vector $|\psi\rangle$, the bra $\langle\psi|$ is defined as the conjugate transpose of $|\psi\rangle$

$$\langle\psi| = (|\psi\rangle)^{\dagger}$$

- $\langle\psi|$ is the row vector you get by transposing $|\psi\rangle$ and taking the conjugate of each of its entries

Example

$$|\psi\rangle = \begin{pmatrix} \frac{1+i}{2} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \implies \langle\psi| = \begin{pmatrix} \frac{1-i}{2} & \frac{1}{\sqrt{2}} \end{pmatrix}$$

- Juxtaposition of a bra and a ket leads to matrix multiplication[2]
- A row vector times a column vector results in a scalar, and
- This scalar will be the **inner product** (or **bracket**) of the vectors involved

Example

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \qquad \text{and} \qquad |\phi\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$$

$$\langle\psi|\phi\rangle \overset{def}{=} \langle\psi|\ |\phi\rangle = (\overline{\alpha}\ \ \overline{\beta}) \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \overline{\alpha}\gamma + \overline{\beta}\delta$$

[2] Interpreting vectors as matrices with only one row or one column

Juxtaposition of Ket and Bra

- What does this imply?

$$|\psi\rangle \langle\phi|$$

Juxtaposition of Ket and Bra

- What does this imply?

$$|\psi\rangle \langle\phi|$$

- A column vector times a row vector gives you a matrix.

Juxtaposition of Ket and Bra

- What does this imply?

$$|\psi\rangle \langle\phi|$$

- A column vector times a row vector gives you a matrix.
- One can easily verify the following:

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

References

1. Quantum Computing for Computer Scientists, by Noson S. Yanofsky, Mirco A. Mannucci
2. Quantum Computing Explained, David Mcmahon. John Wiley & Sons
3. Lecture Notes on Quantum Computation, John Watrous, University of Calgary
    - `https://cs.uwaterloo.ca/~watrous/QC-notes/`