"The Canon"

The Canon refers to a set of fundamental quantum algorithms developed in the early years of Quantum Computing and were the first to establish provable "Quantum advantage"

Query Model

Also known as the "black box". In this model there is an underlying function that is unknown. However, there is a function which can be constructed which can be queried to determine a relationship between input and output. This is called the Oracle O_f

$$O_f|x\rangle = |x \oplus f(x)\rangle$$

$\oplus$ ← addition modulo 2

O_f is unitary (because it is its self-inverse). The oracle can be queried with specific inputs in the quantum register and reversibly write the output to that register

Query model provides a lower bound on the number of steps (gates). Each query is at least one step in the algorithm, so if it can be effectively done with queries, it is effective with gates. Thus query model helps identify fast quantum algorithms

Deutsch - Josza Algorithm

We begin with a simple quantum algorithm due to David Deutsch, discovered in 1985. The generalization of this algorithm is by Bernstein and Vazirani called the Deutsch - Josza algorithm

The problem Deutsch's algorithm tackles is

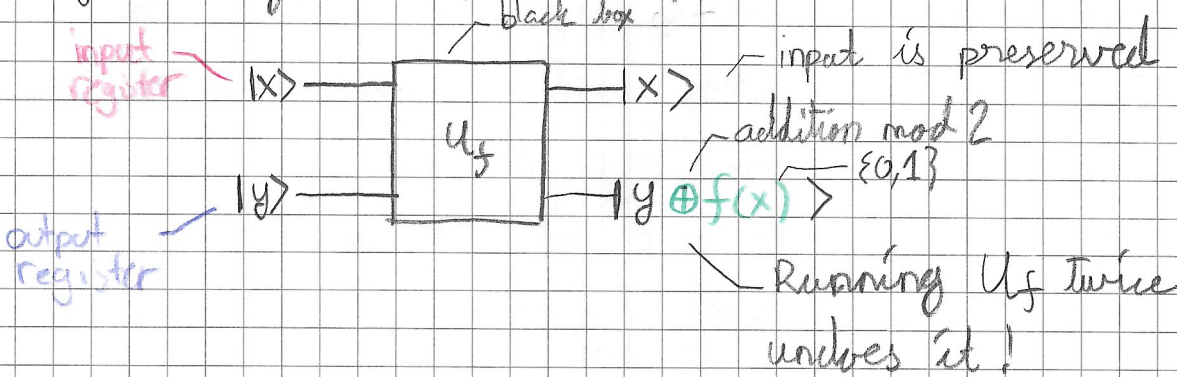
$$f: \{0,1\} \to \{0,1\}$$

where f is unknown (black box). Determine whether f is constant or balanced. Here constant means f always outputs the same bit, i.e $f(0)=f(1)$ and balanced means f outputs different bits on different inputs. i.e. $f(0) \neq f(1)$

The classical way to solve this problem exactly requires application of f two times. With a quantum setup, we need to apply f only once. This is called "Quantum query complexity". Even when we have 9999999 gates, if it queries f two times, the algorithm is said to be of complexity 2, all "non-query" operations are considered free.

Let's begin by putting the f in an unitary form. f by itself is not unitary since when it is constant, it is not invertible to obtain input

We need to put $f(x)$ in a way such that the computation can be undone. This is achieved by casting the $f(x)$ into Oracle



$$|x\rangle|y\rangle \xrightarrow{U_f} |x\rangle|y \oplus f(x)\rangle \xrightarrow{U_f} |x\rangle|y \oplus f(x) \oplus f(x)\rangle$$

$f(x) \oplus f(x) = 0$, $y \oplus 0 = y$

$$= |x\rangle|y\rangle$$

This is the trick we are going to use in order to access any classical function f in quantum framework

$U_f \in U((\mathbb{C}^2)^{\otimes 2})$ is an unitary operator mapping $|x\rangle|y\rangle \longrightarrow |x\rangle|x \oplus y\rangle$ for any $x, y \in \{0,1\}$

A naive approach:

Let's put $|x\rangle$ as $\alpha|0\rangle + \beta|1\rangle$ and $|y\rangle$ as $|0\rangle$ hence putting the input register as a superposition of both states, 0 and 1, and consequently U_f should return a superposition of both possible outputs, $f(0)$ and $f(1)$

$$|\psi\rangle = U_f(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle = \alpha U_f|0\rangle|0\rangle + \beta U_f|1\rangle|0\rangle$$

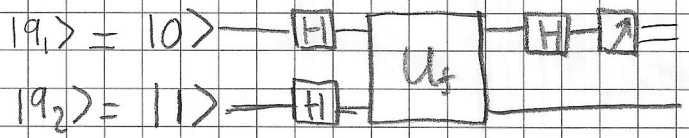
$$= \alpha |0\rangle |f(0)\rangle + \beta |1\rangle |f(1)\rangle$$

We seem to have obtained both outputs with a single query. Unfortunately, we cannot hope to extract both answers with a measurement. Once we measure both registers in the standard basis, we will collapse to one of the two terms in the superposition, effectively destroying the other term.

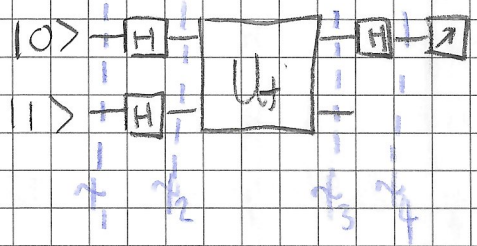
Luckily, our goal is not to extract both $f(0)$ and $f(1)$ after a single query. Rather we want something simpler. Evaluate $f(0) \oplus f(1)$

f is constant $\rightarrow f(0) \oplus f(1) = 0$ f is balanced $\rightarrow f(0) \oplus f(1) = 1$

Deutsch's algorithm



We shall analyse why this circuit works first by brute force, then a second time with an intuitive and elegant Quantum computing trick called the "phase kickback" trick.



$$|\psi_1\rangle = |0\rangle|1\rangle$$

$$|\psi_2\rangle = |+\rangle|-\rangle$$

$$= \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

$$= \frac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle)$$

$$|\psi_3\rangle = \frac{1}{2}\Big(|0\rangle|\overbrace{0\oplus f(0)}^{f(0)}\rangle - |0\rangle|1\oplus f(0)\rangle + |1\rangle|\overbrace{0\oplus f(1)}^{f(1)}\rangle - |1\rangle|1\oplus f(1)\rangle \Big)$$

Case 1 : f constant $\quad f(0) = f(1)$

$$|\psi_3\rangle = \frac{1}{2}\Big(|0\rangle|f(0)\rangle - |0\rangle|1\oplus f(0)\rangle + |1\rangle|f(0)\rangle - |1\rangle|1\oplus f(0)\rangle \Big)$$

$$= \frac{1}{2}\Big((|0\rangle + |1\rangle)\otimes|f(0)\rangle - (|0\rangle + |1\rangle)\otimes|1\oplus f(0)\rangle \Big)$$

$$= \frac{1}{2}(|0\rangle + |1\rangle)\otimes\Big(|f(0)\rangle - |1\oplus f(0)\rangle\Big)$$

$$= \frac{1}{\sqrt{2}}|+\rangle\otimes(|f(0)\rangle - |1\oplus f(0)\rangle)$$

$$|\psi_4\rangle = |0\rangle\otimes\frac{1}{\sqrt{2}}(|f(0)\rangle - |1\oplus f(0)\rangle)$$

↑ measuring gives $|0\rangle$ with certainty

Case 2: f is balanced $\quad (f(0)\neq f(1))$

↳ $f(0) = f(1)\oplus 1$
$f(1) = f(0)\oplus 1$

$$|\psi_3\rangle = \frac{1}{2}(|0\rangle|f(0)\rangle - |0\rangle|f(1)\rangle + |1\rangle|f(1)\rangle - |1\rangle|f(0)\rangle)$$

$$= \frac{1}{2}\Big((|0\rangle - |1\rangle)\otimes|f(0)\rangle - (|0\rangle - |1\rangle)\otimes|f(1)\rangle\Big)$$

$$= \frac{1}{2}(|0\rangle - |1\rangle)\otimes(|f(0)\rangle - |f(1)\rangle)$$

$$= \frac{1}{\sqrt{2}}|-\rangle\otimes(|f(0)\rangle - |f(1)\rangle)$$

Thus qubit 1 is in state $|-\rangle$

$$|\psi_4\rangle = \frac{1}{\sqrt{2}} |1\rangle \otimes (|f(0)\rangle - |f(1)\rangle)$$

hence qubit 1 is exactly at 1 state

conclusion: If f is constant, algorithm outputs 0, if f is balanced, the algorithm outputs 1

The phase kickback trick

Consider what happens when run U_f on input $|x\rangle|-\rangle$

↳ don't matter what

$$|\psi\rangle = U_f |x\rangle|-\rangle = \frac{1}{\sqrt{2}} (U_f|x\rangle|0\rangle - U_f|x\rangle|1\rangle)$$

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

$$= |x\rangle \otimes \frac{1}{\sqrt{2}} (|f(x)\rangle - |1 \oplus f(x)\rangle)$$

there are two cases $f(x)=0$ or $f(x)=1$

$f(x)=0$:

$$|\psi\rangle = |x\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = |x\rangle|-\rangle$$

$f(x)=1$:

$$|\psi\rangle = |x\rangle \otimes \frac{1}{\sqrt{2}} (|1\rangle - |0\rangle) = -|x\rangle|-\rangle$$

→ phase kicked out

i.e. a -1 phase factor is produced

$$U_f|x\rangle|-\rangle = (-1)^{f(x)} |x\rangle|-\rangle$$

phase kickback

↳ eigenvalue ↳ eigenvector

GÜLPAŞ

The answer is encoded in the phase!

Reanalyzing Deutsch's algorithm with phase kickback

$$|\psi_2\rangle = |+\rangle|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|-\rangle + |1\rangle|-\rangle)$$

(no need to expand thanks to phase kickback)

via phase kickback $(|x\rangle|-\rangle \xrightarrow{U_f} (-1)^{f(x)}|x\rangle|-\rangle)$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle|-\rangle + (-1)^{f(1)}|1\rangle|-\rangle\right)$$

case 1: f is constant $f(0)=f(1)$

$$|\psi_3\rangle = (-1)^{f(0)}\frac{1}{\sqrt{2}}(|0\rangle|-\rangle + |1\rangle|-\rangle) = (-1)^{f(0)}|+\rangle|-\rangle$$

$$|\psi_4\rangle = (-1)^{f(0)}|0\rangle|-\rangle$$

→ measure returns 0

→ global phase

case 2: f balanced ie $f(0)\neq f(1)$

up to ± 1 phase

$$|\psi_3\rangle = \pm\frac{1}{\sqrt{2}}(|0\rangle|-\rangle - |1\rangle|-\rangle) = \pm|-\rangle|-\rangle$$

→ global phase

$$|\psi_4\rangle = \pm|1\rangle|-\rangle$$

Measuring returns 1

The Deutsch - Josza Algorithm

Like Deutsch algorithm but for n bits

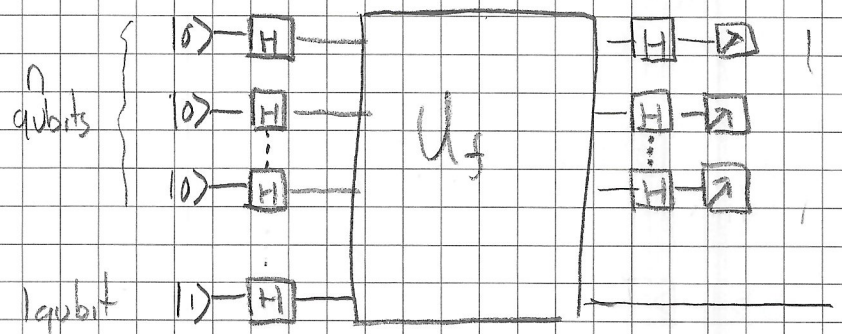
$f\{0,1\}^n \to \{0,1\}$

here constant means $f(x)$ is the same for all $x \in \{0,1\}$ and balanced means $f(x)=0$ for precisely half the $x \in \{0,1\}^n$ and $f(x)=1$ for the rest

The oracle is analogous to Deutsch.

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

where now x is an n-bit state



As before, we divid the computation into 4 stages

Ψ_1 : start of the circuit Ψ_2 : after the Hadamards

Ψ_3 : after U_f Ψ_4 : after last Hadamards

$$|\Psi_1\rangle = |0\rangle \cdots |0\rangle |1\rangle = |0\rangle^{\otimes n} |1\rangle$$

$$|\Psi_2\rangle = |+\rangle \cdots |+\rangle |-\rangle = |+\rangle^{\otimes n} |1\rangle$$

We really have to use phase kickback trick here due to complexity

$$|+\rangle^{\otimes n} = \frac{1}{\sqrt{2}^n} \underbrace{(|0\rangle+|1\rangle) \otimes \cdots \otimes (|0\rangle+|1\rangle)}_{n \text{ brackets}} = \frac{1}{2^{n/2}} \cdots \otimes |1\rangle$$

↳ expansion yields sum over all 2^n bit strings

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

$|P(s)| = \partial^{|s|}$

$$|\psi_2\rangle = |+\rangle^{\otimes n} |1\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle|-\rangle$$

$$|\psi_3\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle|-\rangle$$

$$|\psi_4\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} H^{\otimes n} |x\rangle|-\rangle$$

What is this state?

What $H^{\otimes n}|x\rangle$ equals for arbitrary $x \in \{0,1\}^n$?

Single qubit

$$H|0\rangle = |+\rangle \qquad H|1\rangle = |-\rangle$$

$$H|x_1\rangle = \frac{1}{\sqrt{2}} \sum_{z_1 \in \{0,1\}} (-1)^{x z_1} |z_1\rangle$$

↖ -1 comes out only when $z = |1\rangle$

i.e.

$$H|1\rangle = \frac{1}{\sqrt{2}} \left((-1)^{1\cdot 0} |0\rangle + (-1)^{1\cdot 1} |1\rangle \right)$$

$$= |-\rangle$$

when $|x\rangle = |x_1\rangle|x_2\rangle \cdots |x_n\rangle$

$$H^{\otimes n}|x\rangle = H|x_1\rangle \otimes \cdots \otimes H|x_n\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{z_1 \in \{0,1\}} (-1)^{x_1 z_1} |z_1\rangle \otimes \cdots \otimes \sum_{z_n \in \{0,1\}} (-1)^{x_n z_n} |z_n\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{z \in \{0,1\}^n} (-1)^{x_1 z_1 + \cdots + x_n z_n} |z\rangle$$

GÜLPAŞ

notice that we only care if $x.z$ is even or odd

$$|\psi_4\rangle = \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} H^{\otimes n}|x\rangle|-\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \left(\frac{1}{2^{n/2}} \sum_{z\in\{0,1\}^n} (-1)^{x.z}|z\rangle \right)|-\rangle$$

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

case 1 : constant f

$$|\psi_4\rangle = (-1)^{f(x)} \sum_{z\in\{0,1\}^n} \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x.z} \right)|z\rangle|-\rangle$$

test this with $|z\rangle = |0\rangle\cdots|0\rangle$

$$\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x_0\cdots 0} = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^0$$

$$= \frac{1}{2^n} \sum_{x\in\{0,1\}^n} 1 = \frac{1}{2^n} 2^n = 1$$

$|0\rangle^{\otimes n}|-\rangle$ has amplitude $\underline{1}$, and $\langle\psi_4\rangle = \underline{1}$

hence output when f is constant must be $|0\rangle^{\otimes n}$

case 2 : balanced f

again try $|z\rangle = |0\rangle\cdots|0\rangle$

$$\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)+x.0000} = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}$$

Since $z=0$, Since f is balanced, half is $f(x)=0$ other half is $f(x)=1$, sum cancels out. You can never have this state when f is balanced

GÜLPAŞ