Basics of Linear Algebra in context of Quantum Computing

A quantum state is a 'superposition' of classical states. Mathematically, it is expressed as a vector of amplitudes. Nature has ensured that these amplitudes are complex numbers.

1. Vector Spaces

In our case the field is complex, i.e, $\mathbb{C}$

Def: A vector space V over a field $\mathbb{F}$ is a set of objects called vectors that satisfy the following

- closed under scalar multiplication
  i.e, if $\omega \in V$ and $c \in \mathbb{F}$
  then $c\omega \in V$. This holds for all $\omega \in V$ and all $c \in \mathbb{F}$

- closed under addition
  i.e., if $v, \omega \in V$ then $v + \omega \in V$.
  This holds for all $v, \omega \in V$.

Notation: If V is a vector space of d dimension then $V = \mathbb{F}^d$ which is the set of all column vectors of d elements from $\mathbb{F}$.

For e.g. let $\omega \in V$ and $V = \mathbb{F}^d$ and $\mathbb{F} = \mathbb{C}$ — set of complex numbers

then we can write $\omega = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_d \end{pmatrix}$ where each $c_i \in \mathbb{C}$.

Linearly Independent Vectors :

A set of vectors $v_1, \ldots, v_m \in V$ is 'linearly independent' if $\sum_{i=1}^{m} \alpha_i v_i = 0$ only when

$\alpha_1 = \alpha_2 = \cdots = \alpha_m = 0$.

Span over field $\mathbb{F}$ of set of vectors

$S = \{v_1, v_2, \ldots, v_m\} \subseteq V$ is the set Span(S) that can be written as a linear combination $\sum_{i=1}^{m} \alpha_i v_i$ with coefficients $\alpha_i \in \mathbb{F}$ $\forall i \in [m]$.

Basis for V

(very important to our context)

is a linearly independent set S of vectors such that Span(S) = V.

Exercise 1: Can you give an example of a basis for $V = \mathbb{C}^d$, which is a vector space of d dimension ?

2. Inner Product Space

(There is a general way to define Inner Product space for a vector space over a field $\mathbb{F}$. But we only consider $\mathbb{F} = \mathbb{C}$)

We could add an extra constraint to our vector space to have 'inner product' defined between every vector in the space.

Vector Space + Inner product = Hilbert Space

Inner product between two vectors $v, w \in V = \mathbb{C}^d$ $\mathbb{F}^d$

Suppose $v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_d \end{pmatrix}$ $w = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_d \end{pmatrix}$

Inner product between v & w = $\sum_{i=1}^{d} v_i^* w_i$

(In our complex field v_i^* is complex conjugate of v_i)

But, Inner product between w & v

$$= \sum_{i=1}^{d} w_i^* v_i$$

Note that as for our context $\mathbb{F} = \mathbb{C}$

It is not necessary that $\sum_{i=1}^{d} v_i^* w_i = \sum_{i=1}^{d} w_i^* v_i$

Infact $\langle v|w\rangle = \overline{\langle w|v\rangle}$ → conjugate denoted by $\langle \cdot,\cdot \rangle$

Home Work: Prove it.

So some notations that help us.

To denote a vector $v \in V$ we use $|v\rangle$

↓

Ket Notation

To we use $\langle v|$ to denote the row vector corresponding to v with complex conjugate of each ~~element~~ coordinate in the vector $|v\rangle$

For example. $v \in V = \mathbb{C}^d$

$$v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_d \end{pmatrix} \quad \text{we use} \quad |v\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix}$$

and use $\langle v| = (v_1^* \;\; v_2^* \;\; \ldots \;\; v_d^*)$

Therefore $\langle v|v\rangle = \sum_{i=1}^{d} v_i^* v_i = \|v\|^2$

↓

norm of v.

Hence, $\langle v|v\rangle$ = Square of norm of v.

Let's define a Qubit.

It is a 2-dimensional vector in complex field. with unit norm.

$|\phi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$ where $\alpha_1, \alpha_2 \in \mathbb{C}$

$\langle \phi|\phi\rangle = 1 \Rightarrow \alpha_1^* \alpha_1 + \alpha_2^* \alpha_2 = 1 \Rightarrow |\alpha_1|^2 + |\alpha_2|^2 = 1$.

2 qubits

Consider the Basis for 1 qubit space

$\{|0\rangle, |1\rangle\}$

Now two qubits can be written as.

linear combination of

$\alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle$ with $\sum_{i=1}^{4} |\alpha_i|^2$

where $|00\rangle = |0\rangle \otimes |0\rangle$, similarly for other elements as well.

Exercise 2:

Show that $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ form a basis for vector space expressing 2 qubits.

Also show the basis as Basis vectors.

Exercise 3: Show that a state

$|\phi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ is entangled.

I.e., $|\phi\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle$ for any

$|\psi_A\rangle$ and $|\psi_B\rangle$ in $\mathbb{C}^2$.

Exercise 4: (later exercise!) Show that there exists no unitary U that can clone a state $|\phi\rangle$ in $\mathbb{C}^2$.

I.e., show that it is not possible to have a U s.t $U|\phi\rangle|0\rangle \longrightarrow |\phi\rangle|\phi\rangle$

Hint: Use linearity of U and entanglement pre-definition.

Homework: Show that there is no unitary U that can delete information.

i.e No unitary U exists that does $U|\phi\rangle|\phi\rangle \longrightarrow |\phi\rangle|0\rangle$

Unitary Matrices

To evolve a vector $v \in V \in \mathbb{C}^d$ we use 'unitary' matrices of dimension $d \times d$.

A matrix U is unitary if $U^{-1} = U^{\dagger}$

- U^{-1}: inverse of matrix
- $U^{\dagger}$: Complex Conjugate + Transpose

Some properties

1. $U^{\dagger}U = I$ — Easy to see from the defn.
2. $\langle Uv | Uw \rangle = \langle v | w \rangle$ for all $v, w \in V$ — Preserves Inner Product
3. $\langle Uv | Uv \rangle = \langle v | v \rangle$ for all $v \in V$ — Preserves norm
4. Linearity $U|\alpha u + \beta v\rangle = \alpha U|u\rangle + \beta U|v\rangle$ for all $\alpha, \beta \in \mathbb{C}$ and $u, v \in V$.

Tensor Product

If we have two vector spaces V_A, V_B of dimension d & d' respectively then $V = V_A \otimes V_B$ is a $d \cdot d'$ dimensional vector space.

Additionally if $v \in V_A$ and $w \in V_B$

$$|v\rangle \otimes |w\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix} \otimes \begin{pmatrix} w_1 \\ \vdots \\ w_{d'} \end{pmatrix} = \begin{pmatrix} v_1 w_1 \\ v_1 w_2 \\ \vdots \\ v_1 w_{d'} \\ v_2 w_1 \\ v_2 w_2 \\ \vdots \\ v_d w_1 \\ \vdots \\ v_d w_{d'} \end{pmatrix}$$

$d \cdot d'$ dimensional vector.

Examples of some cute single qubit unitaries

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

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

Example of a 2 qubit unitary

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

$CNOT\ |0b\rangle \longrightarrow |0b\rangle$ Here $b \in \{0,1\}$

$CNOT\ |1b\rangle \longrightarrow |1\bar{b}\rangle$ $\bar{b} = b \oplus 1$, $b \in \{0,1\}$.

Exercise: How to create an EPR pair from $|00\rangle$ state.

EPR pair: $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Exercise: $H \otimes H : |0\rangle|0\rangle \longrightarrow ?$

Exercise: $H^{\otimes n}|i\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{j \in \{0,1\}^n} (-1)^{i.j} |j\rangle$

i is a string $\{0,1\}^n$

Verify this with $n = 3$.

Measurement

If we have a qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$

Measuring this qubit in computational basis ~~gives us~~ collapses the state $|\phi\rangle$ into $|0\rangle$ with probability $|\alpha|^2$.

And collapses $|\phi\rangle$ into $|1\rangle$ with probability $|\beta|^2$.

Recall that qubits have norm 1. Therefore the measurement outcome will always be either $|0\rangle$ or $|1\rangle$.

Similarly, If we had a 2 qubit state

$$|\psi\rangle = \alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle$$

then measuring the 2 qubits in computational basis will ~~give~~ collapse

$|\psi\rangle$ into $|00\rangle$ with probability $|\alpha_1|^2$

$|01\rangle$ with probability $|\alpha_2|^2$

$|10\rangle$ with probability $|\alpha_3|^2$

and

$|11\rangle$ with probability $|\alpha_4|^2$.

But instead of measuring both the qubits but instead you measure, say, the first one then

$$|\psi\rangle = |0\rangle(\alpha_1|0\rangle + \alpha_2|1\rangle) + |1\rangle(\alpha_3|0\rangle + \alpha_4|1\rangle)$$

$$= \sqrt{(|\alpha_1|^2 + |\alpha_2|^2)}\,|0\rangle\left(\frac{\alpha_1|0\rangle + \alpha_2|1\rangle}{\sqrt{|\alpha_1|^2 + |\alpha_2|^2}}\right) + \sqrt{(|\alpha_3|^2 + |\alpha_4|^2)}\,|1\rangle\left(\frac{\alpha_3|0\rangle + \alpha_4|1\rangle}{\sqrt{|\alpha_3|^2 + |\alpha_4|^2}}\right)$$

With probability $|\alpha_1|^2 + |\alpha_2|^2$ we get outcome $|0\rangle$ and state collapses to $|0\rangle\left(\frac{\alpha_1|0\rangle + \alpha_2|1\rangle}{\sqrt{|\alpha_1|^2 + |\alpha_2|^2}}\right)$

with probability $|\alpha_3|^2 + |\alpha_4|^2$ we get outcome $|0\rangle$ and state collapses to $|1\rangle\left(\frac{\alpha_3|0\rangle + \alpha_4|1\rangle}{\sqrt{|\alpha_3|^2 + |\alpha_4|^2}}\right)$

Teleportation Protocol.

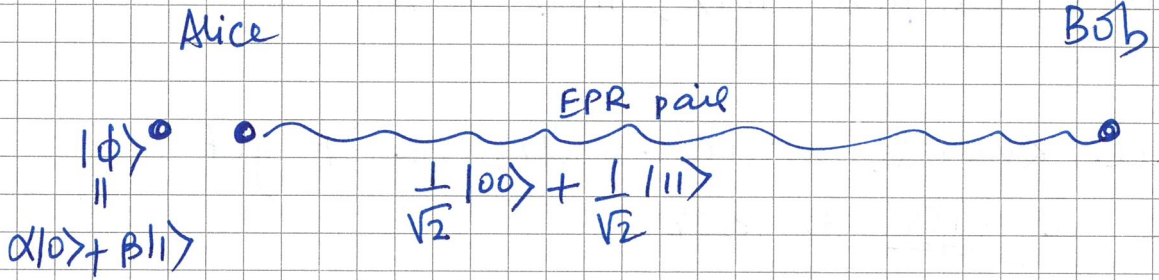
Suppose we have two parties Alice & Bob.
Alice has a qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ for some $\alpha, \beta \in \mathbb{C}$ but Alice doesn't know the values.

Alice wants to send $|\phi\rangle$ to Bob using classical bits

Additionally Alice & Bob share a EPR pair

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Recall that this is an entangled state.



Joint state of Alice and Bob

$$\frac{\alpha}{\sqrt{2}}|\underset{A}{0}\underset{B}{0}0\rangle + \frac{\alpha}{\sqrt{2}}|\underset{A}{0}\underset{B}{1}1\rangle + \frac{\beta}{\sqrt{2}}|\underset{A}{1}\underset{B}{0}0\rangle + \frac{\beta}{\sqrt{2}}|\underset{A}{1}\underset{B}{1}1\rangle$$

↓ Alice performs CNOT

$$\frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|110\rangle + \frac{\beta}{\sqrt{2}}|101\rangle$$

↓ Alice performs H on first qubit

$$\frac{\alpha}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{|1\rangle}{\sqrt{2}}\right)|00\rangle + \frac{\alpha}{\sqrt{2}}\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)|11\rangle + \frac{\beta}{\sqrt{2}}\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)|10\rangle + \frac{\beta}{\sqrt{2}}\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)|01\rangle$$

$$= \frac{\alpha}{2}\left(|000\rangle + |100\rangle + |011\rangle + |111\rangle\right) + \frac{\beta}{2}\left(|010\rangle - |110\rangle + |001\rangle - |101\rangle\right)$$

Rearranging the terms we get

$$\frac{1}{2}|00\rangle(\alpha|0\rangle + \beta|1\rangle)$$
$$+ \frac{1}{2}|01\rangle(\alpha|1\rangle + \beta|0\rangle)$$
$$+ \frac{1}{2}|10\rangle(\alpha|0\rangle - \beta|1\rangle)$$
$$+ \frac{1}{2}|11\rangle(\alpha|1\rangle - \beta|0\rangle)$$

Now Alice Measures in computational basis with probability $\frac{1}{4}$ Alice gets one of the four outcomes $|00\rangle$, $|01\rangle$, $|10\rangle$ or $|11\rangle$

Once Alice knows which outcome it got it sends 2 bits to Bob.

Then Bob knows what to do.
For eg. If Alice gets $|00\rangle$ then Bob has to do nothing. because Bob has $\alpha|0\rangle + \beta|1\rangle$ now.

If Alice gets $|01\rangle$, and tells that to Bob then Bob applies X on its qubit.

If Alice gets $|10\rangle$ and communicates the same to Bob then Bob ~~gets~~ applies Z gate on its qubit.

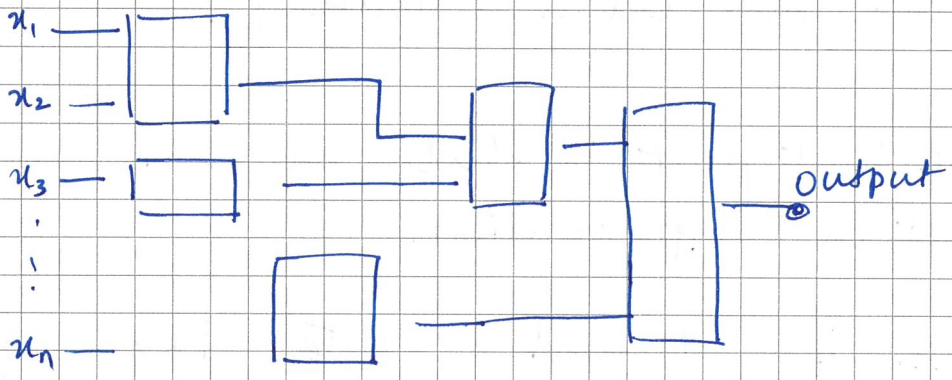
If Alice gets $|11\rangle$ then Bob after knowing that applies X and Z.
Ultimately Bob is able to get state $|\phi\rangle$.

Classical Circuits

A Boolean Circuit is a directed acyclic graph with AND, OR & NOT gates as internal nodes. It has n input nodes and some output nodes. Let us stick to 1 output

We say a Boolean circuit C computes a Boolean function $f: \{0,1\}^n \to \{0,1\}$ if $C(x) = f(x) \quad \forall x \in \{0,1\}^n$.

Eg.



Quantum Circuit also a directed acyclic graph contains ~~m~~ m wires but elementary quantum gates as we discussed earlier.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

But a slightly different model.

Instead of inputs in the wire as we see in the classical circuit we access the input through an 'Oracle' which is a unitary operation.

$$O_x |i, 0\rangle \rightarrow |i, x_i\rangle$$

Bit oracle

where my input is x and $x = x_1 x_2 \ldots x_N \in \{0,1\}^N$ are N bits of my input.

more generally

$$O_x |i, b\rangle \rightarrow |i, b \oplus x_i\rangle$$

Exercise: Show O_x is a unitary.

The best part is that we can access the input in superposition.

For eg. if I had a state $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^{\log n}} |i\rangle$

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_i$$

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle$$

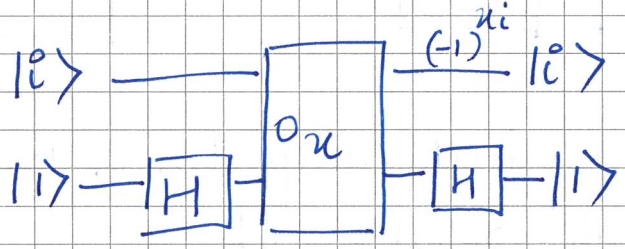
Then $O_x |\psi\rangle|b\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} O_x |i\rangle|b\rangle$

$$= \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle |b \oplus x_i\rangle$$

Phase Oracle.

$$O_{x,\pm}\,|i\rangle \longrightarrow (-1)^{x_i}\,|i\rangle$$

Let's implement a phase oracle from this Bit oracle



$$|i\rangle|1\rangle \xrightarrow{I\otimes H} \frac{|i\rangle}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\downarrow O_x$$

$$O_x\frac{|i\rangle|0\rangle}{\sqrt{2}} \neq -\,O_x\frac{|i\rangle|1\rangle}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2}}\left(|i\rangle|x_i\rangle - |i\rangle|1\oplus x_i\rangle\right)$$

$$= \frac{1}{\sqrt{2}}|i\rangle\left(|0\rangle - |1\rangle\right) \quad \text{if } x_i = 0$$

else

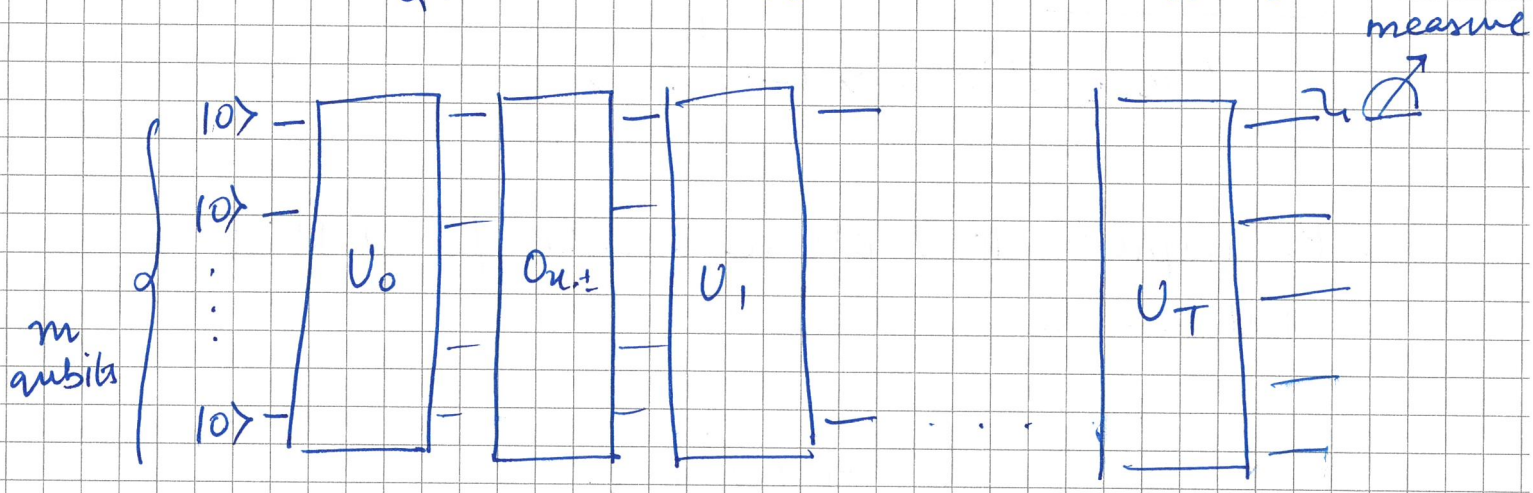
$$\frac{1}{\sqrt{2}}|i\rangle\left(-|0\rangle + |1\rangle\right) \quad \text{if } x_i = 1$$

$$= \frac{1}{\sqrt{2}}(-1)^{x_i}|i\rangle\left(|0\rangle - |1\rangle\right)$$

$$\downarrow I\otimes H$$

$$\frac{1}{\sqrt{2}}(-1)^{x_i}|i\rangle|1\rangle$$

General Quantum Circuit model have



If We say a circuit computes a Boolean function $f: \{0,1\}^n \to \{0,1\}$ iff

$C(x) = f(x)$ with probability $\geq \frac{2}{3}$ $\forall x \in \{0,1\}^n$

Our inputs are given via O_x, the oracles.

Deutsch - Jozsa Problem

Suppose $N = 2^n$, we are given an $x \in \{0,1\}^N$ such that either

1. all x_i have same value ("constant" 0 or 1)
2. $\frac{N}{2}$ of the x_i have 0 and rest are 1 ("balanced").

We want to find out if the given x is constant or balanced.

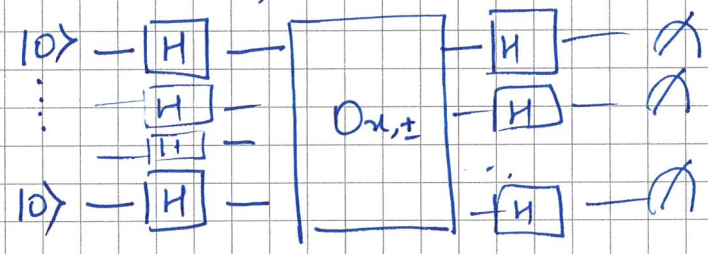
For example let's take $n = 2 \Rightarrow N = 4$

The possible inputs are $\{0000, 1111, 0011, 0101, 1100, 1010, 0110, 1001\}$

Q. Algorithm

We start with an all zero quantum state.

$$|0\rangle^{\otimes n} = \underbrace{|0\rangle|0\rangle \cdots |0\rangle}_{n \text{ of them}}$$



Lets look at this algorithm

$$|0\rangle^{\otimes n} \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle \xrightarrow{O_{x,\pm}} \frac{1}{\sqrt{2^n}} \sum_i (-1)^{x_i} |i\rangle$$

$$\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{x_i} \sum_{j \in \{0,1\}^n} (-1)^{i.j} |j\rangle$$

at $|y\rangle = |0^n\rangle$ state.

$$\frac{1}{2^n} \sum_{i \in \{0,1\}^n} (-1)^{x_i} = \begin{cases} 1 & \text{if } x_i = 0 \text{ for all } i \\ -1 & \text{if } x_i = 1 \text{ for all } i \\ 0 & \text{if } x \text{ is balanced.} \end{cases}$$

Which means by looking at the final state on n qubits we can conclude with certainity if our given x was constant or balanced.

How many queries did we use? Just one! (But in superposition)

Homework: Verify the algorithm for $n = 3$ case

A classical deterministic algorithm needs about $\frac{N}{2} + 1$ queries