Quantum Computation

1994 - Peter Shor - Factoring of an n-digit number with a quantum computer, polinomial in n, ($O(n^2)$)

The best known algorithm for factoring on a regular computer is $O(2^{\sqrt[3]{n}})$ time - (General Number Sieve)

1995 - Grover - Searching.

Topics to be (hopefully) covered:

- Quantum Computation - Algorithms.
- Quantum Information
- Quantum Fault Tolerance - Error - correction.
- Quantum Cryptography - Secure! No need for assumptions about the adversary.

The Model

Classical: Bit : 0, 1 - (can measure it, set to 0 or 1, do NOT)

Probabilistic bit: $\begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$ $p_0+p_1=1$, $p_0, p_1 \geq 0$ (p_0 - probability the bit is 0)

If we measure the bit we get either 0 or 1, and the state collapses (so we won't get different results by measuring it twice)

The operations can be described by matrices. For example:

$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rightarrow NOT \cdot \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} = \begin{pmatrix} p_1 \\ p_0 \end{pmatrix}$

$\text{Set-To-0} : \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \rightarrow \text{Set-To-0} \cdot \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$\text{Randomize} : \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} \rightarrow \text{Rand} \cdot \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$

(we only use stochastic matrices - The sum of each column is 1)

2 bits : Can be similarly described by a vector $\begin{pmatrix} p_{00} \\ p_{01} \\ p_{10} \\ p_{11} \end{pmatrix}$ (and we can extend it to more bits)

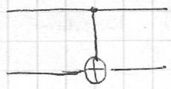
$p = \begin{pmatrix} 1/5 \\ 4/5 \end{pmatrix}$ $q = \begin{pmatrix} 2/3 \\ 1/3 \end{pmatrix}$ $\underbrace{p \otimes q}_{\text{"tensor" of } p \text{ and } q} = \begin{pmatrix} 2/15 \\ 1/15 \\ 8/15 \\ 4/15 \end{pmatrix}$ = the description of 2 bits (p, q)

If we perform NOT on p: $\begin{pmatrix} 8/15 \\ 4/15 \\ 2/15 \\ 1/5 \end{pmatrix} = (NOT \cdot p) \otimes q$

The matrix describing the operation $p \otimes q \longrightarrow (NOT \cdot p) \otimes q$ is therefor:

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \underset{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}{NOT} \otimes \underset{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}{I}$$

<u>CNOT</u> - Controlled Not Operation:



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

$$CNOT \cdot \begin{pmatrix} 8/15 \\ 4/15 \\ 2/15 \\ 1/15 \end{pmatrix} = \begin{pmatrix} 8/15 \\ 4/15 \\ 1/15 \\ 2/15 \end{pmatrix}$$

$\longrightarrow$ measure 1st bit: we get 0 with prob. 12/15 and 1 with 3/15.

$\xrightarrow{0}$ $\begin{pmatrix} 2/3 \\ 1/3 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 2/3 \\ 1/3 \end{pmatrix}$

$\xrightarrow{1}$ $\begin{pmatrix} 0 \\ 0 \\ 1/3 \\ 2/3 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1/3 \\ 2/3 \end{pmatrix}$

<u>Quantum</u>: <u>Qubit</u>: $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$, $\alpha_0, \alpha_1 \in \mathbb{C}$, $\sum_{i=0}^{1} |\alpha_i|^2 = 1$

α_i are called <u>amplitudes</u>. "Probality" of getting 0 is $|\alpha_0|^2$.

The <u>Dirac notation</u> "ket": $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ $|+\rangle = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

$|-\rangle = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ $i \cdot |1\rangle = \begin{pmatrix} 0 \\ i \end{pmatrix}$

Operations on a qubit are represented by unitary matrices:

"NOT" $= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = X$ (X-matrix)

$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = Y$

$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z$

$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H$ (Hadamard-matrix)

<u>Def.</u>: A matrix $U \in \mathbb{C}^{n \times n}$ is called <u>unitary</u> if $U^{\dagger} U = I$ (where $U^{\dagger} = (U^*)^t$) "dagger"

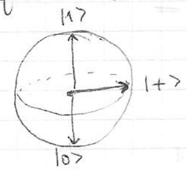
<u>Example</u>: $v \in \mathbb{C}^n$, $U \in \mathbb{C}^{n \times n}$ is unitary $\Rightarrow$ $\left(\langle u, v \rangle = \sum_{i=1}^{n} u_i^* v_i \right)$

$$\|Uv\|_2^2 = \langle Uv, Uv \rangle = (Uv)^{\dagger} \cdot Uv = v^{\dagger} U^{\dagger} U v = v^{\dagger} v = \|v\|_2^2$$

So multiplying by unitary matrices preserves the norm.

* After we measure a qubit, it's state **collapses** to $|0\rangle$ or $|1\rangle$ (depending, of course, on what we measure)

Often qubits are represented as points on a sphere



2 qubits: $|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |0\rangle \otimes |0\rangle \in \mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$

$$|{+}0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |+\rangle \otimes |0\rangle$$

not a tensor product state! $\leftarrow$ $|\text{singlet}\rangle = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} = \dfrac{|01\rangle - |10\rangle}{\sqrt{2}}$

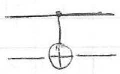
$$\frac{|{+-}\rangle - |{-+}\rangle}{\sqrt{2}} \underset{\substack{\uparrow \\ \text{Check!}}}{=} \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ -1 \\ 1 \\ 0 \end{pmatrix} = -|\text{singlet}\rangle$$

Exercise: Show that for any 2 orthonormal vectors $|u\rangle, |u^\perp\rangle$:

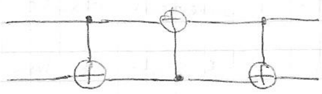
$$\frac{|u u^\perp\rangle - |u^\perp u\rangle}{\sqrt{2}}$$

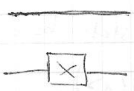
is a singlet up to a global phase ($z \cdot |\text{singlet}\rangle$, $|z| = 1$).

Operations on 2 qubits:

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

Exercise: What is the matrix for the following circuit:



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

* If we measure the 1st qubit of the state:

$$\begin{pmatrix} 1/2 \\ 1/2 \\ 1/2 \\ 1/2 \end{pmatrix} \begin{array}{l} \xrightarrow{0} \text{ with prob. } \tfrac{1}{2} \xrightarrow{\text{collapse}} \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \\ 0 \\ 0 \end{pmatrix} = |0\rangle \otimes |+\rangle \\ \xrightarrow{1} \text{ with prob. } 1/2 \xrightarrow{\text{collapse}} \begin{pmatrix} 0 \\ 0 \\ 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = |1\rangle \otimes |+\rangle \end{array}$$

Quantum Teleportation:

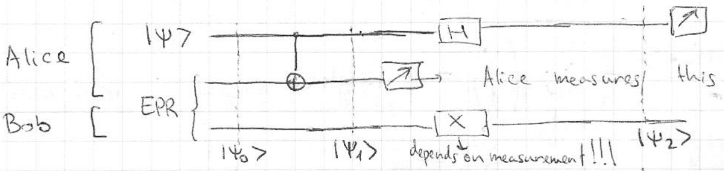
Alice has a qubit: $|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$

(α, β possibly unknown)

We assume Alice & Bob share an EPR state $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$. (Alice has 1st, Bob the 2nd)

$|\psi_0\rangle = |\psi\rangle |EPR\rangle = \frac{1}{\sqrt{2}} \left(\alpha \cdot |0\rangle \cdot (|00\rangle + |11\rangle) + \beta \cdot |1\rangle \, (|00\rangle + |11\rangle) \right)$

it's common not to write $\otimes$



* It is impossible to duplicate quantum states! So the state will disappear from Alice and appear for Bob.

$|\psi_0\rangle = \frac{1}{\sqrt{2}} \left(\alpha |000\rangle + \alpha |011\rangle + \beta |100\rangle + \beta |111\rangle \right)$

$|\psi_1\rangle = \frac{1}{\sqrt{2}} \cdot \left(\alpha \cdot |000\rangle + \alpha |011\rangle + \beta \cdot |110\rangle + \beta |101\rangle \right)$

Alice measures 2nd qubit.

if 0: the state becomes $\alpha \cdot |000\rangle + \beta |101\rangle$. After omitting 2nd qubit, we get $\alpha \cdot |00\rangle + \beta \cdot |11\rangle$.

(see that both happen with prob. 1/2)

if 1: the state becomes $\alpha \cdot |01\rangle + \beta \cdot |10\rangle$

Alice tells Bob (over the phone) the masurement result. If it's 1, Bob applies an X gate on the 3rd qubit. The state is then always be $\alpha \cdot |00\rangle + \beta \cdot |11\rangle$.

Use Hadamard on $|\psi\rangle$. The new state becomes:

$|\psi_2\rangle = \frac{1}{\sqrt{2}} \left(\alpha |00\rangle + \alpha |10\rangle + \beta |01\rangle - \beta |11\rangle \right)$.

Alice measures 1st qubit:

if 0: the state becomes $\alpha |0\rangle + \beta |1\rangle = |\psi\rangle$ ~~for the~~

if 1: the state becomes $\alpha |0\rangle - \beta |1\rangle$.