QUANTUM COMPUTING

Carlile Lavor

clavor@ime.unicamp.br

UNICAMP, Brazil

1 The postulates of quantum mechanics

- **Postulate 1:** there is a complex vector space with inner product associated to any closed physical system, where a state of this system is described by a unit vector.

- System: Quantum Bit (qubit)

- Vector Space: $\underline{\mathbb{C}^2}$

- An orthonormal basis for $\mathbb{C}^2$ can be given by $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$, which will be represented by the Dirac notation:

$$\begin{aligned} |0\rangle &= \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \\ |1\rangle &= \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \end{aligned}$$

- A general state $|\psi\rangle$ of a qubit can be given by

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where $|\alpha|^2 + |\beta|^2 = 1$ $(\alpha, \beta \in \mathbb{C})$.

- The basis $\{|0\rangle, |1\rangle\}$ is called the <u>computational basis</u> and the vector $|\psi\rangle$ is called a <u>superposition</u> of the states $|0\rangle$ and $|1\rangle$, with <u>amplitudes</u> α and β.

- **Postulate 2:** the evolution of a closed quantum system is described by a linear operator which preserves the inner product (unitary operator). That is,

$$|\psi_2\rangle = U|\psi_1\rangle,$$

where $|\psi_1\rangle$ is the state of the system at time t_1, $|\psi_2\rangle$ is the state at time t_2, and U is a unitary operator.

- There is a unitary operator which transforms $|0\rangle$ in $|1\rangle$ and vice versa. It is denoted by X and its matrix representation, in the computational basis, is given by

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

- Another example is the operator Z:

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

- It is easy to see that

$$X|0\rangle = |1\rangle,$$

$$Z|0\rangle = |0\rangle,$$

  and, for $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$,

$$\begin{aligned} X|\psi\rangle &= \beta|0\rangle + \alpha|1\rangle, \\ Z|\psi\rangle &= \alpha|0\rangle - \beta|1\rangle. \end{aligned}$$

- However, note that for the Hadamard operator, given by

$$H = \frac{1}{2^{1/2}} \left[\begin{array}{rr} 1 & 1 \\ 1 & -1 \end{array} \right],$$

  we obtain

$$H|0\rangle = \frac{1}{2^{1/2}}(|0\rangle + |1\rangle).$$

- The dual of $|\varphi\rangle \in \mathbb{C}^2$, denoted by $\langle\varphi|$, is defined by

$$\langle\varphi| = |\varphi\rangle^\dagger.$$

- Given $|\varphi\rangle, |\psi\rangle \in \mathbb{C}^2$, the inner product $\langle\varphi|\psi\rangle$ and the outer product $|\varphi\rangle\langle\psi|$ are defined, respectively, by

$$\begin{aligned} \langle\varphi|\psi\rangle &= |\varphi\rangle^\dagger|\psi\rangle, \\ |\varphi\rangle\langle\psi| &= |\varphi\rangle|\psi\rangle^\dagger. \end{aligned}$$

- <u>Example</u>:

$$\langle 0|1\rangle = 0$$

and

$$|0\rangle\langle 1| = \left[\begin{array}{cc} 0 & 1 \\ 0 & 0 \end{array}\right].$$

- **Postulate 3:** a measurement of a quantum system is described by a <u>hermitian operator</u> M ($M^\dagger = M$), where the possible outcomes of the measurement correspond to the eigenvalues λ_i of M.

- Upon measuring the state $|\psi\rangle$, the probability of getting result λ_i is given by

  $$p_{\lambda_i} = \langle\psi|(|i\rangle\langle i|)|\psi\rangle,$$

  where $\{|i\rangle\}$ is an orthonormal basis of eigenvectors associated to $\{\lambda_i\}$.

- Given that outcome λ_i occured, the state of the system immediately after the measurement is

  $$|\psi_{\lambda_i}\rangle = \frac{(|i\rangle\langle i|)|\psi\rangle}{p_{\lambda_i}^{1/2}}.$$

- Example: consider the hermitian operator Z,

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

which can be written as

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|.$$

- Suppose that the state being measured is

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

Then,

$$\begin{aligned} p_1 &= |\alpha|^2, \\ |\psi_1\rangle &= \frac{\alpha}{|\alpha|}|0\rangle, \end{aligned}$$

and

$$\begin{aligned} p_{-1} &= |\beta|^2, \\ |\psi_{-1}\rangle &= \frac{\beta}{|\beta|}|1\rangle. \end{aligned}$$

- **Postulate 4**: the joint state of a system with components $|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_n\rangle$ is the tensor product $|\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle$.

- For $A \in \mathbb{C}^{m \times n}$ and $B \in \mathbb{C}^{p \times q}$, we define the tensor product $A \otimes B$ by:

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix}.$$

- Example:

$$|0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

and

$$|1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

2 Grover´s algorithm

- Problem: given an unstructured list with N element, find a specific one.

- Suppose that the list is $\{0, 1, ..., N-1\}$, where $N = 2^n$, and that the function that recognizes the searched element i_0 is given by
  $$f : \{0, 1, ..., N-1\} \rightarrow \{0, 1\},$$
  where
  $$f(i) = \left\{ \begin{array}{l} 1, \text{ if } i = i_0 \\ 0, \text{ if } i \neq i_0 \end{array} \right. .$$

3 The first Grover´s operator

- For each element of the list $\{0, 1, ..., N-1\}$, we associate the state $|i\rangle_n$ of n qubits.

- We search for an operator U_f which transforms $|i\rangle_n$ into $|f(i)\rangle_1$.

- Since U_f must be unitary, consider

$$|i\rangle_n|0\rangle_1 \xrightarrow{U_f} |i\rangle_n|f(i)\rangle_1.$$

- Then,

$$U_f\left(|i\rangle|0\rangle\right)=\left\{\begin{array}{l}|i\rangle|1\rangle,\ \text{if } i=i_0\\ |i\rangle|0\rangle,\ \text{if } i\neq i_0\end{array}\right. .$$

- If the second register is $|1\rangle$, we define

$$U_f\left(|i\rangle|1\rangle\right)=\left\{\begin{array}{l}|i\rangle|0\rangle,\ \text{se } i=i_0\\ |i\rangle|1\rangle,\ \text{se } i\neq i_0\end{array}\right. .$$

- In a more compact form, we have

$$U_f\left(|i\rangle|j\rangle\right)=|i\rangle|j\oplus f(i)\rangle,$$

  where $\oplus$ is the sum modulo 2 (note that $U_f \in \mathbb{C}^{2^{n+1}\times 2^{n+1}}$).

4 Superposition of the elements of $\{0, 1, ..., N-1\}$

- The first and second registers are initialized on the states $|0\rangle_n$ and $|1\rangle_1$, respectively.

- If we apply the operator H on each qubit of these registers, we obtain that

$$|\psi\rangle = (H|0\rangle)^{\otimes n} = \frac{1}{2^{n/2}} \sum_{i=0}^{2^n-1} |i\rangle$$

and

$$|-\rangle = H|1\rangle = \frac{1}{2^{1/2}}(|0\rangle - |1\rangle).$$

- Now, applying the operator U_f on $|\psi\rangle|-\rangle$, we get

$$U_f\left(|\psi\rangle|-\rangle\right) = \left(\frac{1}{N^{1/2}} \sum_{i=0}^{N-1} (-1)^{f(i)}|i\rangle\right)|-\rangle.$$

5 The second Grover´s operator

- The next step should be to increase the amplitude of the searched element, which can be obtained using another unitary operator defined by

$$2|\psi\rangle\langle\psi| - I.$$

- Applying this operator on the state

$$\frac{1}{N^{1/2}}\sum_{i=0}^{N-1}(-1)^{f(i)}|i\rangle$$

  and measuring the first register, the probability of getting the searched element is

$$\left|\frac{3N-4}{N^{3/2}}\right|^2.$$

- The composition of the operators U_f and $2|\psi\rangle\langle\psi| - I$ is called Grover´s operator G, that is,

$$G = ((2|\psi\rangle\langle\psi| - I) \otimes I)\, U_f.$$

6 Complexity of Grover´s algorithm

- It can be proved that the resulting action of the operator G^k ($k \in \mathbb{N}$) rotates $|\psi\rangle$ towards $|i_0\rangle$ by $k\theta$ rad, in the subspace spanned by $|\psi\rangle$ and $|i_0\rangle$, where θ is the angle between $|\psi\rangle$ and $G|\psi\rangle$.

- It can also be proved that the number of times k that the operator G must be applied so that the angle between $|i_0\rangle$ and $G^k|\psi\rangle$ becomes zero is

$$k = \arccos\left(\frac{1}{N}\right)\left(\arccos\left(\frac{N-2}{N}\right)\right)^{-1},$$

which implies that

$$\lim_{N\to\infty} \frac{k}{N^{1/2}} = \frac{\pi}{4} \Rightarrow k = O(N^{1/2}).$$