Quantum Computing

Part I: Basic Principles

Jamal Slim

FTX - SFT Group

jamal.slim@desy.de

Regular Group Meeting
September 15, 2022

Presentation Overview

- Basic concepts
- formal| informal definitions
- Some algebra
- Quantum registers
- Quantum entanglement and Bell states
- Basic quantum gates

- In a classical computer, a bit is a representation of a physical quantity with two states.
  - e.g., voltage, magnetization, charge density.
- In a quantum computer, the concept of a quantum bit or qubit is used.
  - Similar to the classical bit, each qubit refer to two distinct states.
  - The principles of orthogonality, superposition and entanglement are borrowed from QM.

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$
$$|\Psi\rangle = \alpha\,|\uparrow\rangle + \beta\,|\downarrow\rangle$$

Concepts - Cont

Classical and quantum

- Orthogonality
  - qubits cannot exist with 100% certainty at the same time.
- Superposition
  - a qubit may have many other states which are the superposition of the two distinct states
  - calculations on multiple basis states at the same time, (not possible in classical computing).
  - example of superposition in classical mechanics light polarization.
- Other aspects such as:
  - reversibility, robustness.

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

Quantum computing: Definitions

- Quantum computing can be described as a manipulation of vectors through operations in a vector space spanned by the distinct vector (basis)
  - Vectors are manipulated through special quantum gates (operations).
  - These operations are just rotations of vectors in hyperspaces with well-defined inner product (Hilbert spaces).

Quantum computing: Definitions - Cont

- A vector is a state of a physical system, e.g., electron spin $|\Psi\rangle = \alpha\,|\uparrow\rangle + \beta\,|\downarrow\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Let the electron spin space, which can be spanned by the $|\uparrow\rangle\,|\downarrow\rangle$ basis vectors if we choose to do so.
- $|\uparrow\rangle\,|\downarrow\rangle$ are not real space direction vector like $\vec{\mathrm{e}}_{\mathrm{z}}$ and $-\vec{\mathrm{e}}_{\mathrm{z}}$.
- $|\uparrow\rangle\,|\downarrow\rangle$ do not have a direct relationship with the up and down vectors in the real space
- $|\uparrow\rangle \neq -\,|\downarrow\rangle$
- Other basis vectors such as $|\leftarrow\rangle\,|\rightarrow\rangle$ can be chosen
- Basis transformation is allowed

Quantum computing: Definitions - Cont

- Any quantum mechanical state is a vector and it is a linear combination of the basis vectors in a given basis.
- A basis formed by the basis states corresponding to an observable is a convenient choice in the formulation of the quantum computing problems.
- Two formalism from QM
  - Wave mechanics - Schrödinger Equation.
  - Matrix Quantum Mechanics (MQM) - particularly powerful when combined with Dirac's bra–ket notation
- Using MQM, the evolution of a quantum state is represented by an operator which is represented by a matrix (Pauli matrices)

Copenhagen Interpretation

- If an observable corresponding to a self-adjoint operator (i.e. Hermitian) M with discrete spectrum, measured in a system with normalized state Ψ , then
  - The result will be one of the eigenvalues $= \lambda_{\mathrm{i}}$ of M.
  - The probability is $\langle\Psi|\,\mathrm{P_i}\,|\Psi\rangle$, where $\mathrm{P_i}$ is projection operator to project any state to the subspace of $|\mathrm{i}\rangle$, ($\mathrm{P_i} = |\mathrm{i}\rangle\,\langle\mathrm{i}|$, or tensor product).

Some Linear Algebra Postulates

- QC operators represented by a matrix U must be unitary.
- The column vectors of any unitary matrix are orthonormal to each other.
- An orthonormal set of basis vectors transformed by a matrix, U , if it is still orthonormal, then U must be unitary.
- If two vectors (states) are transformed by the same unitary matrix, their inner product is preserved.
- If all the vectors (states) are transformed by the same unitary vector, it is equivalent to transforming the coordinates in the opposite "direction".

Quantum Register

- First, for QC, knowledge of the detailed implementation is not required.
- 1-qubit of information $|\mathrm{a}\rangle$ represents a vector in the $\mathbb{C}^2$ space, $|\mathrm{a}\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$.
- If $|\mathrm{a}\rangle = |0\rangle$ or $|\mathrm{a}\rangle = |1\rangle$, the quantum register stores exactly the same information as the classical one, This is the most direct relationship between the quantum register and the classical register. If the quantum register is only allowed to store the basis states, it is the same as a classical register.
- An n-qubit register stores information in $\mathbb{C}^{\mathrm{n}} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$, a simple grouping of qubits.
- The quantum register does store only the basis states (which is equivalent to the capability of a classical register), but the linear combination of the basis states. And the number of basis states, thus the dimension of the Hilbert space, grows exponentially with the number of qubits.

Quantum Data Processing

- A n-qubit register stores a 2^{n}-dimensional space vector. (e.g. for n= 100, only 100 (polarized) electrons. Classically, to store a 2^{100} dimensional space vector, it is needed to store its 2^{100} complex coefficients.
- Using the linearity and superposition of QM, the calculations of the basis states can be done simultaneously: quantum parallelism.

$$|\Psi\rangle = \alpha\,|\uparrow\uparrow\rangle + \beta\,|\uparrow\downarrow\rangle + \gamma + \beta\,|\downarrow\uparrow\rangle + \delta\,|\downarrow\downarrow\rangle =$$

$$\alpha\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\\0\\0\end{pmatrix} + \gamma\begin{pmatrix}0\\0\\1\\0\end{pmatrix} + \delta\begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma + \beta\,|10\rangle + \delta\,|11\rangle$$

Entanglement

- Let $|\mathrm{a}\rangle$, $|\mathrm{b}\rangle$ and $|\mathrm{c}\rangle$ be vectors related such that $|\mathrm{a}\rangle = \sum_{\mathrm{j}=1}^{\mathrm{n}} |\mathrm{b_j}\rangle \otimes |\mathrm{c_j}\rangle$
- It is possible that for some higher-dimensional vectors, to be expressed as one single tensor product of two lower-dimensional vectors, each from a lower-dimensional space, i.e., if $\mathrm{n} = 1$, these vectors are unentangled, aka., seperable or product state, otherwise, they are entangled.
- Example:

$$|h\rangle = |f\rangle \otimes |g\rangle$$

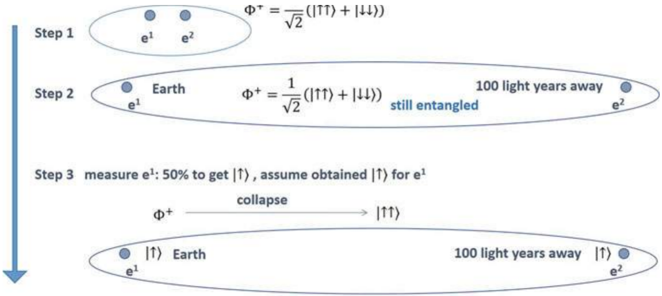
$$= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \qquad = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

Entanglement: Bell states

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}; \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}; \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}$$

- Example

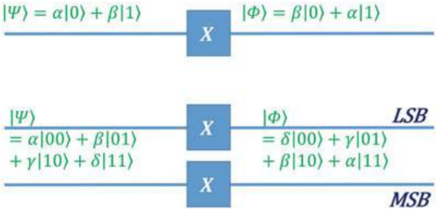


Quantum Gate

- Again, QC is a series of unitary rotations of a high- dimensional vector in a high-dimensional space with preserved inner product.
- Every evolution is a unitary, reversible rotation.
- A quantum gate is a gate that performs a unitary operation.
- In QC, usually, the qubit and its "signal" do not flow in the space. Instead, we apply operations such as microwave or laser pulses to operate/manipulate/change the qubit. Therefore, the flow of a quantum algorithm usually represents the flow of time instead of a physical layout in the space

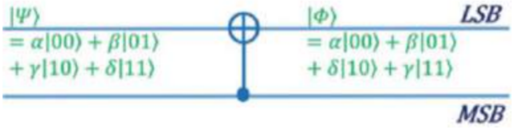
NOT (X) Gate

- Let $\mathrm{U_N}$ be the rotation matrix of the quantum gate given that $\mathrm{U_N}\left|0\right\rangle = \left|1\right\rangle$ and $\mathrm{U_N}\left|1\right\rangle = \left|0\right\rangle$. $\mathrm{U_X}$ reads
$\mathrm{U_N} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$



XOR (CNOT) Gate

- XOR quantum gate is 2-qubit gate with rotation matrix $\mathrm{U_X}$
  $\mathrm{U_X}\,|\mathrm{ab}\rangle = |\mathrm{aa} \oplus \mathrm{b}\rangle$, with $\oplus$ being the classical XOR sum.
  $\mathrm{U_X}\,|00\rangle = |0, 0 \oplus 0\rangle = |0, 0\rangle = |00\rangle$
  $\mathrm{U_X}\,|01\rangle = |0, 0 \oplus 1\rangle = |0, 1\rangle = |01\rangle$
  $\mathrm{U_X}\,|10\rangle = |1, 1 \oplus 0\rangle = |1, 1\rangle = |11\rangle$
  $\mathrm{U_X}\,|11\rangle = |1, 1 \oplus 0\rangle = |1, 0\rangle = |10\rangle$
  $$\mathrm{U_X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



The End

Questions? Comments?