Theory of Quantum Information and Quantum Computing

Maso*

October 4, 2024

Contents

Lecture 1

mer 02 ott 2024 16:30

Topics. A review of quantum mechanics. The first part is about qubits and the theory behind them: entanglement, Bell's inequalities. In this part one defines the operation of the quantum computer, define quantum gates; one defines algorithms and looks for the ones that are faster than classical ones; Shor's algorithm and others. Quantum error correction (not done: fault tolerance). The second part is about the physical realization of quantum computers: ion traps and superconducting qubits. A qubit is just a two-level quantum system: for ion traps the two levels are two well-separated excitation modes of an ion. The superconducting qubits are also called artificial atoms: they are made from superconducting circuits, there is no resistance and the circuit behaves as an harmonic oscillator.

Knowledge required. Quantum mechanics from the bachelor.

References. Main reference is the Nielsen–Chuang, "Quantum computation and quantum information". It is a compendium, not really technical and not written for physicists. For quantum computation and quantum algorithms there is Mermin, "Quantum computer science". Some online lectures are: Aaronson at Austin University for educated general audiences, Preskill at Caltech (fault tolerance), IBM webpage.

For the second part of the course, see professor's notes and refs online.

Currently there are several quantum computers. The first quantum computer was based on quantum annealing which is good for optimization problems, but this is not treated in the course. The course studies the superconducting qubits at IBM and Google. Right now, the order of qubits is about a thousand and not much can be done. The majority of those qubits are allocated for error correction. The problem with qubits is transfer the classical information to the two levels in an isolated way. It is difficult to keep stable an excitation and it is even more difficult to maintain a superposition with a given relative phase. With time, the phases get washed out by the interactions with the environment. Keeping coherence of a two-level quantum system is difficult.

Exam. The exam is just an oral evaluation. Can be done whenever with enough notice. If one wishes, one may give a presentation about a topic not done in the course; the questions are more general; the presentation must be agreed upon.

---

*`https://github.com/M-a-s-o/notes`

1 Meccanica quantistica

Notation. The state of the two-level system are called

$$|0\rangle \ , \quad |1\rangle$$

One considers these two states as carriers of information: the quantum analog of the classic bit. The main difference between classical and quantum computation is that quantum state may exist in superposition

$$\alpha\,|0\rangle + \beta\,|1\rangle \ , \quad \alpha, \beta \in \mathbb{C}$$

Quantum mechanics is inherently probabilistic. If the system is in the state $|0\rangle$, then, by performing a measurement to see in which state the system is, one finds $|0\rangle$. One may state with certainty that the system is in the state $|0\rangle$. Same for $|1\rangle$. However, if the state is in a superposition, it is not obvious in which state the system is. One may find either state with probability

$$P(|0\rangle) = |\alpha|^2 \, , \quad P(|1\rangle) = |\beta|^2$$

If the two above are probabilities, then it must hold

$$|\alpha|^2 + |\beta|^2 = 1$$

From Quantum Mechanics, one knows that the global phase is irrelevant. [r] therefore there are two real numbers that characterizes the state. The quantum states carry a lot of information, the information related to two real numbers. Even if the two numbers are real which in theory may encode everything, the amount of information one may extract is much lower. One extracts the state, not the number. The two numbers may be recovered by performing many measurements on the system. This is true with a large number of initial states, but for a quantum computer there is a single quantum object. When performing a measurement, the wave function collapses and instantly becomes the state just observed. For a single measurement, the outcome must be either state and one may not do another measurement to extract the probabilities: it is impossible to extract the information.

The collapse of the wave function is a very discussed topic in physics. The collapse may be used in quantum computers, one exploits it to extract some information in a clever way.

1.1 Postulates

Definition 1.1 (I, State)**.** In quantum mechanics, states are rays in a Hilbert space.

Let $|\psi\rangle \in \mathcal{H}$ be a vector in the Hilbert space $\mathcal{H}$. A ray is the equivalence class given by

$$|\psi\rangle \sim \mathrm{e}^{\mathrm{i}\alpha}\,|\psi\rangle$$

with $|\psi\rangle$ having unit length.

Remark 1.2. Notice that not all states in the Hilbert space is a good quantum state. One needs to normalize it.

Dirac notation. The scalar product of two states is a complex number

$$\langle\phi|\psi\rangle \in \mathbb{C}$$

The length is defined as

$$\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle}$$

The Hilbert space is a vector space, therefore given two vectors, every linear combination of them is also a vector in the Hilbert space.

The bra $\langle\phi|$ is a covector, a functional that acts on vectors

$$\langle\phi| : \mathcal{H} \to \mathbb{C} \, , \quad |\psi\rangle \mapsto \langle\phi|\psi\rangle$$

For a single qubit, one needs a Hilbert space of dimension 2. All vector spaces of dimension 2 are isomorphic to $\mathcal{H} \simeq \mathbb{C}^2$. One identifies

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

The generic vector is a pair of complex numbers linear combination of the two previous ones

$$\begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = z_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + z_2 \begin{bmatrix} 0 \\ 1 \end{bmatrix} = z_1 |0\rangle + z_2 |1\rangle$$

The scalar product between two arbitrary vectors

$$|\phi\rangle = \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} , \quad |\psi\rangle = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix}$$

is the typical Hermitian scalar product

$$\langle\phi|\psi\rangle = w_1^* z_1 + w_2^* z_2 = \begin{bmatrix} w_1^* & w_2^* \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \end{bmatrix}$$

One identifies

$$\langle\phi| = \begin{bmatrix} w_1^* & w_2^* \end{bmatrix} = (|\phi\rangle)^\dagger$$

The two vectors $|0\rangle$ and $|1\rangle$ have been chosen to be an orthonormal basis of the Hilbert space

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

Form of a generic state. The most general state of a qubit is a generic ray in the Hilbert space. Therefore, one requires that

$$|z_1|^2 + |z_2|^2 = 1$$

There is a convenient parametrization of the parameters

$$|\psi\rangle = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \cos\frac{\theta}{2} e^{i\phi_1} |0\rangle + \sin\frac{\theta}{2} e^{i\phi_2} |1\rangle$$

Applying phase invariance, one may eliminate a phase

$$|\psi\rangle = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \sin\frac{\theta}{2} |0\rangle + \cos\frac{\theta}{2} e^{i\phi} |1\rangle$$

This is not the only way, but it is the typical one.

As noted before, one needs two real numbers to describe the content of the qubit.

Bloch sphere. Consider unit vector in $\mathbb{R}^3$

$$\mathbf{n} = \begin{bmatrix} \sin\theta\cos\varphi \\ \sin\theta\sin\varphi \\ \cos\theta \end{bmatrix} , \quad \theta \in [0, \pi] \,, \quad \varphi \in [0, 2\pi]$$

One covers all possible points on the surface of a sphere. The angle θ is the colatitude and φ is the longitude. There is a parallel between the state of a qubit and a point on this Bloch sphere. The state $|0\rangle$ corresponds to $\theta = 0$, the north pole; while $|1\rangle$ corresponds to $\theta = \pi$. The mapping between the Hilbert space and the Bloch sphere is not an isometry due to the half angle present.

Definition 1.3 (II, Observables)**.** The observables correspond to self-adjoint operators

$$A^\dagger = A$$

where the adjoint is the transpose conjugate $A^\dagger = (A^\top)^* = (A^*)^\top$.

Theorem 1.4 (Spectral)**.** Let A be a self-adjoint operator on a Hilbert space. It exists an orthonormal basis of eigenvectors of such operator

$$A |n\rangle = a_n |n\rangle \,, \quad \langle n|m\rangle = \delta_{nm}$$

Therefore, any vector may be written in terms of the basis

$$|\psi\rangle = \sum_n \alpha_n |n\rangle \,, \quad \alpha \in \mathbb{C}$$

Projection operator. A self-adjoint operator of dimension d has d eigenvalues (not necessarily different). If the eigenvalues are not all different, then there is a degeneracy and one may group the corresponding eigenvectors. For each block, one may define the projection operator

$$P_{a_p} |\psi\rangle = \alpha_{p_1} |p_1\rangle + \cdots + \alpha_{p_n} |p_n\rangle$$

Example 1.5. Consider just one eigenvalue α_n that is not degenerate. The projection of the state $|\psi\rangle$ is done along the eigenvector $|n\rangle$ to give

$$|n\rangle \langle n|\psi\rangle = P |\psi\rangle$$

The second factor is a complex number. One may formally write that

$$P_{\alpha_n} = |n\rangle\langle n|$$

Qubit. [r] In $\mathbb{C}^2$, therefore a qubit, one may parametrize a self-adjoint matrix as

$$A = \begin{bmatrix} a+b & c-\mathrm{i}d \\ c+\mathrm{i}d & a-d \end{bmatrix} = aI + b\sigma_3 + c\sigma_1 + d\sigma_2$$

where σ_i are the Pauli matrices

$$X = \sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} , \quad Y = \sigma_2 = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix} , \quad Z = \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

The two states $|0\rangle$ and $|1\rangle$ are two eigenvectors of σ_3:

$$\sigma_3 |0\rangle = |0\rangle \ , \quad \sigma_3 |1\rangle = -|1\rangle$$

[r] If σ_3 is an observable, there must be an eigenbasis. One may check that the eigenbasis of σ_1 is given by

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} , \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

The eigenbasis of σ_2 is given by

$$|+\mathrm{i}\rangle = \frac{|0\rangle + \mathrm{i}\,|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ \mathrm{i} \end{bmatrix} , \quad |-\mathrm{i}\rangle = \frac{|0\rangle - \mathrm{i}\,|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -\mathrm{i} \end{bmatrix}$$

On the Bloch sphere, the eigenvectors of σ_i lie on the axis i. For a generic point on the sphere, one may define the spin in a generic direction

$$\boldsymbol{\sigma} \cdot \mathbf{n} = \sigma_1 n_1 + \sigma_2 n_2 + \sigma_3 n_3$$

the generic state $|\psi\rangle$ is an eigenvector

$$\boldsymbol{\sigma} \cdot \mathbf{n} \, |\psi\rangle = |\psi\rangle$$