Introduction to Quantum Computing

Qubit representation

Quantum computing uses the Dirac notation for vectors, $|\cdot\rangle$ is called a "ket" and $\langle\cdot|$ a "bra", they correspond respectively to column and row vectors. The bra is the complex conjugate of the ket, meaning that $|\cdot\rangle = \langle\cdot|^\dagger$. The symbol $\dagger$ is a "dagger" and it stands for the complex transpose. A qubit is a $2D$ complex vector living in an Hilbert space $\mathcal{H}$ of basis $\{|0\rangle, |1\rangle\}$. The matrix representation of $|0\rangle$ and $|1\rangle$ are:

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

A qubit is a linear combination of those basis states:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \text{ with } |\alpha|^2 + |\beta|^2 = 1$$

The probabilities of measuring $|0\rangle$ and $|1\rangle$ are $|\alpha|^2$ and $|\beta|^2$. Here are some additional notations:

1. Scalar product: $\langle u|v\rangle$
2. Multiplication with matrix M: $M|u\rangle$
3. Matrix notation: $|u\rangle\langle v|$

The state of a qubit can be expressed as:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle \text{ with } \theta \in [0, 2\pi], \phi \in [0, 2\pi[$$

This gives a 3D representation called the Bloch Sphere:

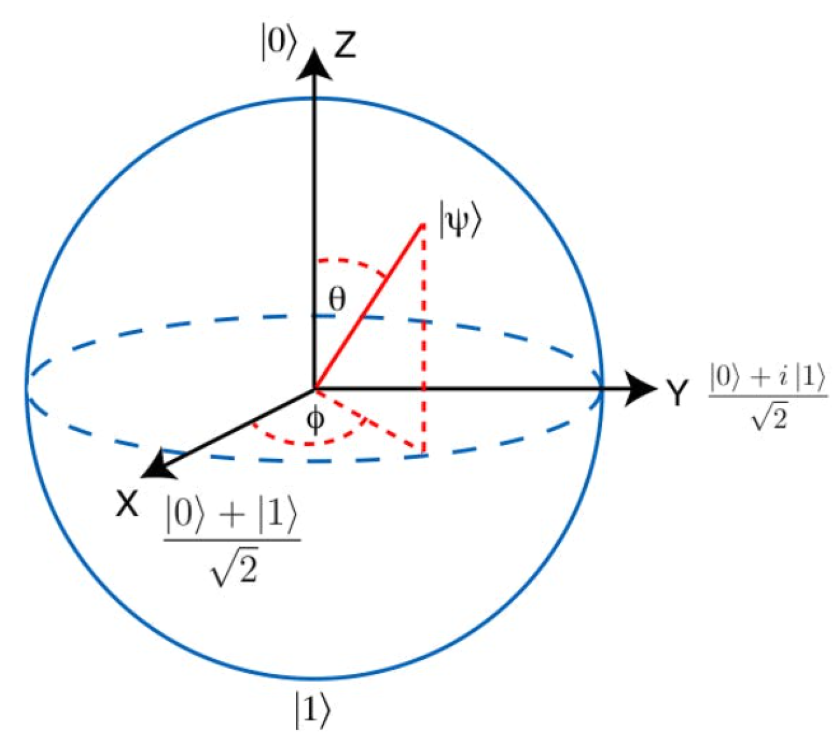


Figure 1. Bloch Sphere: Visual representation of a qubit state.

A quantum system of n qubits has 2^n dimensions and lives in the Hilbert space $\mathcal{H}^{\otimes n} = \mathcal{H}_n \otimes \cdots \otimes \mathcal{H}_1$ of basis $\{|k\rangle\}_{k=0,\dots,2^n-1}$. Note that the writing of k is in binary, as an example we have $|k=4\rangle = |100\rangle$. Thus, in such a space a quantum state reads:

$$\begin{aligned}|\psi\rangle &= \sum_{k_n,\dots,k_1\in\{0,1\}^n} \alpha_{k_n,\dots,k_1}\cdot|k_n\rangle\otimes\cdots\otimes|k_1\rangle\\ &= \sum_{k=0}^{2^n-1}\alpha_k|k\rangle\\ &= \begin{bmatrix}\alpha_0\\ \vdots\\ \alpha_{2^n-1}\end{bmatrix}\end{aligned}$$

with $\sum_{k=0}^{2^n-1}|\alpha_k|^2 = 1$. The symbol $\otimes$ is the Kronecker (tensor) product defined as

$$\begin{aligned}|u\rangle\otimes|v\rangle &= (\alpha_0|0_u\rangle + \alpha_1|1_u\rangle)\otimes(\beta_0|0_v\rangle + \beta_1|1_v\rangle)\\ &= \alpha_0\beta_0|0_u0_v\rangle + \alpha_0\beta_1|0_u1_v\rangle + \alpha_1\beta_0|1_u0_v\rangle + \alpha_1\beta_1|1_u1_v\rangle\\ &= \begin{bmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_0\\ \alpha_1\beta_1\end{bmatrix}\end{aligned}$$

Quantum operations

In quantum computing, all the operations are reversible in a specific way, they are unitary. A matrix M is unitary if its inverse is equal to its conjugate transpose: $MM^\dagger = M^\dagger M = \mathbb{I}$. Here are some really usefull single qubit matrices in quantum computations:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \quad T = \begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$$

The Pauli matrices:

$$X = \sigma_x = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \quad Y = \sigma_y = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} \quad Z = \sigma_z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

The most general form for a single qubit unitary is:

$$U(\theta,\phi,\lambda) = \begin{bmatrix}\cos\frac{\theta}{2} & -e^{i\lambda}\sin\frac{\theta}{2}\\ e^{i\phi}\sin\frac{\theta}{2} & e^{i(\phi+\lambda)}\cos\frac{\theta}{2}\end{bmatrix} \text{ with } \theta\in[0,\pi], (\phi,\lambda)\in[0,2\pi[^2$$

In quantum computation, it is possible to apply a gate on a given qubit if another is in state $|0\rangle$ or $|1\rangle$. The most usefull one is the CNOT gate, it performs the X (NOT) gate on the second qubit if the first one is in state $|1\rangle$:

$$CNOT = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} = \begin{bmatrix}\mathbb{I} & 0\\ 0 & X\end{bmatrix}$$

To act on n qubits, one needs to use $2^n\times 2^n$ unitary matrices. The tensor product for matrices is defined as:

$$A\otimes B = \begin{bmatrix}a_{11}\begin{bmatrix}b_{11}&b_{12}\\b_{21}&b_{22}\end{bmatrix} & a_{12}\begin{bmatrix}b_{11}&b_{12}\\b_{21}&b_{22}\end{bmatrix}\\ a_{21}\begin{bmatrix}b_{11}&b_{12}\\b_{21}&b_{22}\end{bmatrix} & a_{22}\begin{bmatrix}b_{11}&b_{12}\\b_{21}&b_{22}\end{bmatrix}\end{bmatrix} = \begin{bmatrix}a_{11}b_{11}&a_{11}b_{12}&a_{12}b_{11}&a_{12}b_{12}\\ a_{11}b_{21}&a_{11}b_{22}&a_{12}b_{21}&a_{12}b_{22}\\ a_{21}b_{11}&a_{21}b_{12}&a_{22}b_{11}&a_{22}b_{12}\\ a_{21}b_{21}&a_{21}b_{22}&a_{22}b_{21}&a_{22}b_{22}\end{bmatrix}$$

To prepare a set of n qubits in an equal superposition of all the basis states, one has to apply a Hadamard gate on each qubit. As those gates act on separate qubits they can be executed all at once in parallel.

$$H^{\otimes n}(\underbrace{|0\rangle\otimes\cdots\otimes|0\rangle}_{n}) = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle$$

Generally speaking, if the n qubits are in an arbitrary state $|\psi\rangle = |x_1\rangle\otimes\cdots\otimes|x_n\rangle$, the Hadamard tower acts as:

$$H^{\otimes n}|\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}(-1)^{k\cdot x}|k\rangle$$

with $k\cdot x = k_1x_1\oplus\cdots\oplus k_nx_n$, where $\oplus$ is the addition modulo 2 and k_i the i-th bit in the binary writing of k.

Quantum measurement

Performing a measurement on a quantum state makes it collapse. It is possible to measure the entire system or only a part of it. If we perform a measurement on all the qubits of the following state:

$$|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

The probability of measuring each basis state is $|\frac{1}{2}|^2 = \frac{1}{4}$. If the outcome of the measurement is $|01\rangle$, the state becomes $|\psi\rangle = |01\rangle$. Note that we renormalized it. If we did a partial measurement on the first qubit and got $|1\rangle$, the state of the system would have been:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle)$$

Entanglement

Entanglement is a quantum phenomena that can happend with 2 or more qubits, it is used to correlate information in quantum computing. If n qubits are entangled, they form a unique system, meaning that it is impossible to express the state of the system by expressing the state of each qubit separately (with a tensor product). With two qubits, the most entangled state is the Bell state:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}$$

It is not possible to decompose this state with a tensor product of the two qubits composing it. On the other hand, the following state is not entangled as one can decompose it as a tensor product of the two qubits:

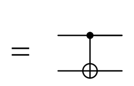
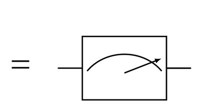
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle\otimes\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Quantum circuit

The most common way to express quantum algorithms are quantum circuits. Here are the basic convention for quantum circuits:

1. The time evolution is from left to right
2. Each line represent a qubit state
3. Boxes put on n qubits are quantum gates acting on those qubits
4. A double line represent a classical state
5. The vertical concatenation denotes a tensor product
6. The horizontal concatenation denotes a composition of operations
7. If not precised, we assume that all qubits start the computation in the $|0\rangle$ state

Here are some symbol used:

1. X =
2. CNOT = 
3. Measurement = 

Let's represent the computation of a state $|00\rangle$ into the Bell state $|\Psi\rangle$:

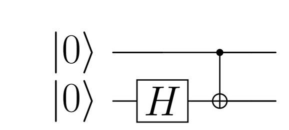


Figure 2. Quantum circuit for 2 qubits.

An interesting circuit is that of Quantum Teleportation as it involves partial measurements:

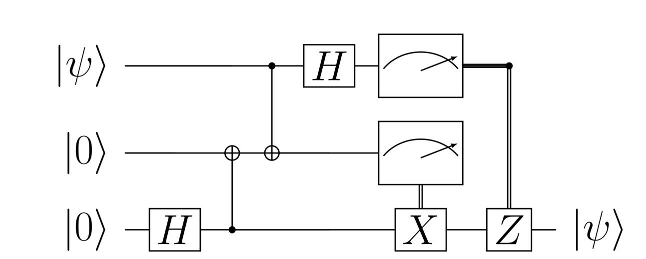


Figure 3. Quantum circuit implementing the Quantum Teleportation protocol.