Quantum Computing (量子计)

Get ready to grasp the leading edge technologies

Driss BOUTAT

Institut National des Sciences Appliquées Centre Val de Loire .

Introduction

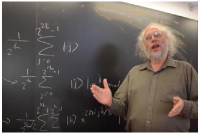
Fourier.

Hadamard.

Fermat.

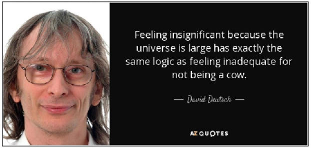
Pauli.

Introduction



Shor.

Jozsa.



Feeling insignificant because the universe is large has exactly the same logic as feeling inadequate for not being a cow.

— David Deutsch —

AZ QUOTES

Deutsch.

Introduction

Binary Computation that rely in binary 0's and 1's or OFF and ON. The state space of Binary Computation are the fields $\mathbb{Z}_2^n$ where $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ with coefficients binary 0's and 1's.

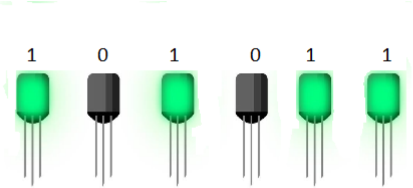


Figure: Binary digits (bits).

Introduction

Binary computation uses the following logical gates in its circuits:

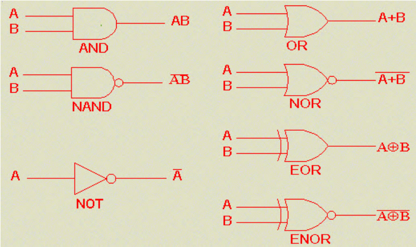


Figure: Logical gates.

Introduction

The realm of Quantum Computation is the world of atomic and subatomic particles. In this tiny world things seem to behave in unexpected way that looked weird even for the most famous physicists of our history. Amid these odd phenomena, we can point out superposition (叠加态) and entanglement (纠缠态) particles can have more state than one state at a time. This fact is the so-called superposition.

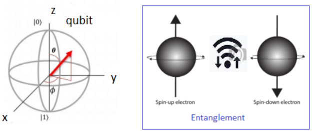


Figure: Bolch Sphere of Qubits left, and entanglement right.

In addition, two particles that interact with each other may share some (secret) things called waves so that if we separate them, they still have an effect on each other. This fact is called entanglement.

Recall on binary basis case

In classically binary computation with n bits, we can write any integer x between 0 and $N = 2^n - 1$ as:

$$\sum_{k=1}^{n} x_k \times 2^{n-k},$$

where x_k are 0's or 1's. We denote it as $x = x_1 ... x_n$. Thus

$$x = x_1 \begin{pmatrix} 1 & 0 & ... & 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 & 1 & ... & 0 \end{pmatrix} + \cdots + x_n \begin{pmatrix} 0 & 0 & ... & 1 \end{pmatrix}$$

thus we work in the space $\mathbb{Z}_2^n$

Thus, for $n = 3$ we work in $\mathbb{Z}_2^3$ that is spanned by three elements: $x = x_1(100) + x_2(010) + x_3(001)$ where x_k are 0's or 1's, $100 = 2^2$, $010 = 2^1$ and $001 = 2^0$.

For example, $7 = 1(100) + 1(010) + 1(001) = 111$ in binary basis.

Recall on binary basis case

By the same way we can also write the fractional numbers (分数) as:

$$0.x_1 ... x_n = \sum_{k=1}^{n} x_k \times \frac{1}{2^k},$$

where x_k are 0's or 1's.

For the example of $n = 3$,

$$0.101 = 1 \times \frac{1}{2} + 0 \times \frac{1}{2^2} + 1 \times \frac{1}{2^3} = \frac{5}{8}.$$

Quantum realm: Quantum basis

If we have n qubits then the quantum realm is

$$\mathcal{H}_2^{\otimes n} = \mathcal{H}_2 \otimes \mathcal{H}_2 ... \otimes \mathcal{H}_2,$$

where $\mathcal{H}_2 = \mathbb{C}^2$ stands for two copies of complex numbers plan.

A quantum state $|\psi\rangle \in \mathcal{H}_2^{\otimes n}$ is such that

$$|\psi\rangle = \sum_{k=0}^{2^n-1} \alpha_k |k\rangle .$$

where $\alpha_k \in \mathbb{C}$ such that $\sum_{k=0}^{2^n-1} |\alpha_k|^2 = 1$ and $|k\rangle$ are the **basis state** (基态). The $|k\rangle$ notation is pronounced kit k. It was introduced by Dirac.

Quantum realm: Quantum basis

What it means $|k\rangle$ is a **basis state** for $k = 0 : 2^n - 1$ with $n = 1$?.
It means two basis states that span $\mathcal{H}_2$:

spin up qubit: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, spin down qubit: $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

For $n = 2$, there are four basis states that span $\mathcal{H}_2 \otimes \mathcal{H}_2$:

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Quantum realm: Quantum basis

Now, for $n = 2$, let's us build the basis $|k\rangle$ for $k = 0 : 2^2 - 1$ of $\mathcal{H}_2^{\otimes 2}$ from the basis of $\mathcal{H}_2$.

- $k = 0$ its writing in binary basis is $k = 00$, therefore its kit is as follows

$$|0\rangle = |00\rangle = |0\rangle \otimes |0\rangle .$$

- $k = 1$ in binary basis is $k = 01$, thus its kit is as follows

$$|1\rangle = |01\rangle = |0\rangle \otimes |1\rangle .$$

- $k = 2$ has its binary form as $k = 10$ and its kit is written as

$$|2\rangle = |10\rangle = |1\rangle \otimes |0\rangle .$$

- $k = 3$ in binary basis has the form $k = 11$ and its kit is given by

$$|3\rangle = |11\rangle = |1\rangle \otimes |1\rangle .$$

Quantum realm: Quantum basis

Let's provide the **tensor product** (张量积)

Definition

The tensor product of two states $|a\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ and $|b\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$ of $\mathcal{H}_2$ is a state in $\mathcal{H}_2 \otimes \mathcal{H}_2$ (which is isomorphic to $\mathbb{C}^4$) given by

$$|ab\rangle = |a\rangle \otimes |b\rangle = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix}$$

Exercise: given $|0\rangle = 0\,|0\rangle + 1\,|1\rangle$ and $|1\rangle = 0\,|0\rangle + 1\,|1\rangle$, check the definition of $|k\rangle \otimes |j\rangle$ with $k, j = 0, 1$ given in the previous slide.

Quantum realm: Quantum basis

Remark

Tensor product is similar to the usual product but not commutative

$$\begin{aligned} |a\rangle \otimes |b\rangle &= (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\gamma\,|0\rangle + \delta\,|1\rangle) \\ &= \alpha\gamma\,|00\rangle + \alpha\delta\,|01\rangle + \beta\gamma\,|10\rangle + \beta\delta\,|11\rangle\,. \end{aligned}$$

where we respect the fact that

$$|kj\rangle = |k\rangle \otimes |j\rangle \neq |j\rangle \otimes |k\rangle = |jk\rangle$$

where $j \neq k$ are 0's or 1's.

Quantum realm: Entanglement

The element of $\mathcal{H}_2 \otimes \mathcal{H}_2$ are not always in the form of $|a\rangle \otimes |b\rangle$. As examples we have the so-called Bell's basis.

Bell's Basis

$$\left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

$$\left|\psi^+\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right).$$

They are states of modulus 1 and they are **orthogonal** thus their scalar product is 0. They span the space $\mathcal{H}_2 \otimes \mathcal{H}_2$.

Quantum realm: Entanglement

We say that state $|\phi\rangle$ is **entangled** (纠缠的) if it can't be written as tensor product of states. Thus $|\phi\rangle \neq |a\rangle \otimes |b\rangle$.

The entanglement plays an important role on the so-called non-cloning of states (量子态的不可复制性), information teleporation (信息传递) in quantum computation and therefore in encryption systems (加密系统).

Let check for example that the following Bell state is entangled

$$\left|\phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right).$$

To achieve this we assume that $\left|\phi^{+}\right\rangle = |a\rangle \otimes |b\rangle$ where $|a\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ and $|b\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$. From this, it stems that $\alpha\gamma = \frac{1}{\sqrt{2}}$, $\beta\delta = \frac{1}{\sqrt{2}}$, $\alpha\delta = 0$ and $\beta\gamma = 0$. This equations lead to a discrepancy.

The scalar product : Bar-Kit

Scalar product (标量积)

The scalar product of two states $|a\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|b\rangle = \gamma|0\rangle + \delta|1\rangle$ is a complex number 复数 given by

$$\langle a| \, |b\rangle = \alpha^*\gamma + \beta^*\delta.$$

where $\langle a|$ is the conjugate transpose or Hermitian transpose (共轭转置) of $|a\rangle$ pronounced the bras of a. So that the norm of the state $|a\rangle$ is given by $\| \, |a\rangle \, \| = \sqrt{\langle a| \, |a\rangle} = \sqrt{|\alpha|^2 + |\beta|^2}$ which equals to 1 because the quantum state has norm 1, we call it **unitary**.

What is the norm of $|ab\rangle$? Factorize:

$$|\alpha\gamma|^2 + |\alpha\delta|^2 + |\beta\gamma|^2 + |\beta\delta|^2 = 1.$$

Thankfully the tensor product respects the unitary property.

Operators on a single qubit

An operator on single qubit is an **unitary matrix** $U : \mathcal{H}_2 \to \mathcal{H}_2$ that satisfies

$$UU^\dagger = U^\dagger U = I_2$$

where I_2 is the identity matrix and $U^\dagger$ is conjugate transpose of U.

Pauli's operators

- $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, thus $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$. It behaves as the logic NOT operator in the binary computation.
- $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, thus $Y|0\rangle = i|1\rangle$ and $Y|1\rangle = -i|0\rangle$, where $i^2 = -1$.
- $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, thus $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$. Thus it changes the phase of the second qubit

Operators on a single qubit

An operator on single qubit is an unitary matrix $U : \mathcal{H}_2 \rightarrow \mathcal{H}_2$. Thus $UU^\dagger = U^\dagger U = I_2$ where I_2 is the identity and $U^\dagger$ is conjugate transpose or Hermitian transpose of U.

Hadamard's operator: superposition

$H = \frac{1}{\sqrt{2}} \left(\begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array} \right)$. The Hadamard's operator provides a **superposition** (**叠加态**) of a given state as follows:
$H\left|0\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right)$ and $H\left|1\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle - \left|1\right\rangle\right)$

Operators decomposition

Let's consider an unitary matrix $U : \mathcal{H}_2 \to \mathcal{H}_2$. Then, it can be decomposed in the following form

Theorem

$$U = e^{i\xi} \begin{pmatrix} e^{i\frac{\alpha}{2}} & 0 \\ 0 & e^{-i\frac{\alpha}{2}} \end{pmatrix} \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \begin{pmatrix} e^{i\frac{\beta}{2}} & 0 \\ 0 & e^{-i\frac{\beta}{2}} \end{pmatrix}.$$

Let set $R_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$ and $R_z(\beta) = \begin{pmatrix} e^{i\frac{\beta}{2}} & 0 \\ 0 & e^{-i\frac{\beta}{2}} \end{pmatrix}$ then we can write $U = e^{i\xi} R_z(\alpha) R_y(\delta) R_z(\beta)$. Where $e^{i\xi} = \det(U)$ is the whole phase.

Operators decomposition

The proof of the previous Theorem stems from the fact that $UU^\dagger = U^\dagger U = I_2$ and $U = \begin{pmatrix} u & -v \\ v^* & u^* \end{pmatrix}$, where * stands for the complex conjugate.

The Pauli's operator and the Hadamard's operator can be obtained as follows

- Set $\xi = \frac{3\pi}{2}$, $\alpha = 0$, $\theta = \frac{\pi}{2}$ and $\beta = \pi$ to get X,
- Set $\xi = \frac{\pi}{2}$ and $\theta = \frac{\pi}{2}$ to get Y.
- $\xi = \frac{3\pi}{2}$, $\alpha = 0$, $\theta = 0$ and $\beta = \pi$ to get Z,
- Set $\xi = \frac{3\pi}{2}$, $\alpha = 0$, $\theta = \frac{\pi}{4}$ and $\beta = \pi$ to get H.

Operators on multiple qubits

Let U_1 and U_2 two unitary operators on $\mathcal{H}_2$, then we can construct an operator U on $\mathcal{H}_4 = \mathcal{H}_2 \otimes \mathcal{H}_2$ as follows

$$U\left(|ab\rangle\right) = U_1 \otimes U_2\left(|a\rangle \otimes |b\rangle\right) = U_1\,|a\rangle \otimes U_2\,|b\rangle\,.$$

Let's provide some examples

- $I_2 \otimes X\left(|01\rangle\right) = |00\rangle$
- $H \otimes H\left(|01\rangle\right) = \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right)$.

Quantum Fourier Transform: QFT

Fourier Transform (傅里叶变换) is on of the most important operator in quantum computation. It's the key of many algorithm implementation. It's a generalization of Hadamard's operator. Let consider n qubits and set $N = 2^n$ then $\omega = e^{\frac{2\pi i}{N}}$ is an N^{th} root of unity. Now the QFT is defined on a basis state $|k\rangle$ as follows:

Definition of QFT (量子傅里叶变换)

$$\mathfrak{F}\,|k\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{N-1} e^{\frac{2i\pi}{2^n}k.j}\,|j\rangle\,.$$

Therefore its matrix picture is given as follows

$$\mathfrak{F} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{(N-1)} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(N-1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \omega^{(N-1)} & \omega^{2(N-1)} & \dots & \omega^{(N-1)(N-1)} \end{pmatrix}$$

Quantum Fourier Transform: QFT

Let show how we can implement it. For this let $j = j_1 .... j_n$ an integer in its binary script. Thus $j = j_1 2^{n-1} + j_2 2^{n-2} + ... + x_{n-1} 2 + j_n$, where j_k are 0's or 1's. Therefore $\frac{j}{N} = 0.j_1 ... j_n = \sum\limits_{k=1}^{n} \frac{j_k}{2^k}$. Then we have

$\mathfrak{F}|x\rangle = \frac{1}{\sqrt{N}} \sum\limits_{j_1=0}^{1} ... \sum\limits_{j_n=0}^{1} e^{2i\pi x.\sum\limits_{k=1}^{n} \frac{j_k}{2^k}} |j\rangle = \frac{1}{\sqrt{N}} \sum\limits_{j_1=0}^{1} ... \sum\limits_{j_n=0}^{1} e^{2i\pi x.\frac{j_m}{2^m}} |j\rangle = \frac{1}{\sqrt{N}} \bigotimes\limits_{m=1}^{n} \left(|0\rangle + e^{\frac{2i\pi x}{2^m}} |1\rangle \right)$. As $\frac{x}{2^m} = x_1 2^{n-1-m} + ... + x_{n-m} + x_{n-m+1}\frac{1}{2} + ... + x_n \frac{1}{2^m}$ has an integer part and and a decimal part, we get

Actionable writing

$$\mathfrak{F}|x\rangle = \frac{1}{\sqrt{N}} \left(|0\rangle + e^{2\pi i \times 0.x_n} |1\rangle \right) \otimes ... \otimes \left(|0\rangle + e^{2\pi i \times 0.x_1 x_2 ... x_n} |1\rangle \right)$$

Quantum Fourier Transform: QFT

As you can see if $n = 1$ the

- $\mathfrak{F}\left|0\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right)$, because $x = 00$ and $0.0 = 0$
- $\mathfrak{F}\left|1\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle - \left|1\right\rangle\right)$, because $x = 01$ and $0.1 = \frac{1}{2}$

Thereby we have $\mathfrak{F} = H$. Set $\theta_k = 2\pi \times 0.x_k x_{k+1} ... x_n = 2\pi\left(\frac{x_k}{2} + \frac{x_{k+1}}{2^2} + ... + \frac{x_n}{2^{n-k+1}}\right)$ such that $e^{i\theta_k} = e^{i\frac{2x_k\pi}{2}} e^{i\frac{2x_{k+1}\pi}{2^2}} ... e^{i\frac{2x_n\pi}{2^{n-k+1}}} = e^{ix_k\pi} e^{i\frac{x_{k+1}\pi}{2}} ... e^{i\frac{x_n\pi}{2^{n-k}}}$. As a composition of rotations where if for some $x_m = 0$ it does not interfere in the calculation. Quantum Fourier Transform can also be presented as follows

Definition of QFT

$$\mathfrak{F}\left|x\right\rangle = \frac{1}{\sqrt{N}}\Big(\left|0\right\rangle + e^{i\theta_n}\left|1\right\rangle\Big)\Big(\left|0\right\rangle + e^{i\theta_{n-1}}\left|1\right\rangle\Big) ... \Big(\left|0\right\rangle + e^{i\theta_1}\left|1\right\rangle\Big)$$

Let's analyse factor by factor

- First factor is

Quantum Fourier Transform: QFT

- Second factor is $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi x_{n-1}} e^{i\frac{\pi x_n}{2}} |1\rangle\right) =$ $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\frac{\pi x_n}{2}} (-1)^{x_{n-1}} |1\rangle\right) = R_{n-1,n} H |x_{n-1}\rangle$ where $R_{n-1,n} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi x_n}{2}} \end{pmatrix}$.
- k^{th} factor is

$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\frac{x_{k+1}}{2}} ... e^{i\frac{x_n}{2^{n-k}}} (-1)^{x_k} |1\rangle\right)$$

$$= R_{k,k+1} R_{k,k+2} ... R_{k,n} H |x_k\rangle .$$

where $R_{k,j} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi x_j}{2^{j-k}}} \end{pmatrix}$ which is identity if $x_j = 0$ and if $x_j = 1$ then it keeps the state $|0\rangle$ unchangeable and rotate the state $|1\rangle$ by angle $\frac{\pi}{2^{j-k}}$.

Quantum Fourier Transform: QFT

The circuit of QFT is as follows

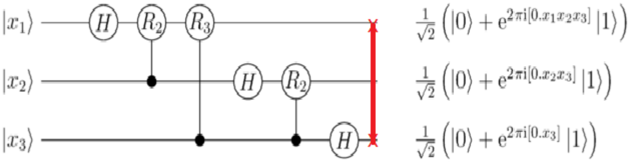

$|x_1\rangle$
$|x_2\rangle$
$|x_3\rangle$
H
R_2
R_3
H
R_2
H
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_1x_2x_3]}|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_2x_3]}|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_3]}|1\rangle\right)$

Figure: QFT Circuit

Quantum Fourier Transform: QFT

If you already know the so-called Discrete Fast or Fourier Transform (DFF or FFT) you well wonder what is the link with QFT?

To answer your concern, we start from the QFT definition

$$\mathfrak{F}\left|x\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{\frac{2i\pi}{2^n} x.y} \left|y\right\rangle .$$

The inverse transform is given by

$$\mathfrak{F}\left|x\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{-\frac{2i\pi}{2^n} x.y} \left|y\right\rangle .$$

and its circuit is devised by running the QFT circuit backwards, and replacing each gate with its inverse.