PHY365: Quantum Information

QiLin Xue

Fall 2021

Contents

1 Overview of Quantum Computing

1.1 Quantum Coins

Consider a quantum coin that can be in a superposition of heads and tails. We can write its state as a vector:

$$|\Psi\rangle = \alpha|H\rangle + \beta|T\rangle \tag{1.1}$$

which lives in the **Hilbert Space.** Inner products of these vectors can be written as

$$\langle\Psi_1|\Psi_2\rangle. \tag{1.2}$$

Born's Rule tells us we can compute the probability of tails to be $|\beta|^2$ and the probability of heads is $|\alpha|^2$. When there are two quantum coins, there can be four combinations of heads and tails, written as:

$$|\Psi\rangle = \alpha|HH\rangle + \beta|HT\rangle + \gamma TH\rangle + \delta|TT\rangle. \tag{1.3}$$

In quantum mechanics, we can construct the following state:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|HH\rangle + \frac{1}{\sqrt{2}}|TT\rangle, \tag{1.4}$$

which represents **entanglement.** If we measure the first coin, we can instantly know the outcome of the second coin, even if they are lightyears apart.

1.2 Building a Better Computer

How might we use quantum coins to help us build a "better" computer? Before we begin to understand and answer this question, let us understand some key concepts.

First, we can measure **information** as the number of bits (binary digits) that are needed to specify a message. Each bit in a computer requires a physical system that has two possible configurations.

- In semiconductor circuits, we use voltage.
- Magnetization is sometimes also used (i.e. in hard drives).
- Pits in optical storage.
- Paper tape with holes in it

Now let's extend the idea to quantum bits, i.e. **qubits**. Let us use $|0\rangle$ and $|1\rangle$ to represent the two possible states of a quantum coin, and we can write a qubit as

$$|\Psi_1\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.5}$$

which isn't necessarily interesting. If we have two qubits, we can write the state as

$$|\Psi_2\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle, \tag{1.6}$$

where the following notation are equivalent:

$$|00\rangle = |0\rangle|0\rangle = |0\rangle \otimes |0\rangle \tag{1.7}$$

where $\otimes$ is the **tensor product** of two vectors. To make it easier to write, we can also write it as:

$$|\Psi_2\rangle = \alpha|0_2\rangle + \beta|1_2\rangle + \gamma|2_2\rangle + \delta|3_2\rangle. \tag{1.8}$$

For three qubits, we have

$$|\Psi_3\rangle = \alpha|000\rangle + \beta|001\rangle + \gamma|010\rangle + \delta|011\rangle + \epsilon|100\rangle + \zeta|101\rangle + \eta|110\rangle + \theta|111\rangle. \tag{1.9}$$

Therefore, N qubits will have 2^N possible states. This suggests that quantum memory can get big, fast.

1.2.1 Quantum Parallelism

However, this is not the only difference. Each qubit operation, i.e. $|0\rangle \longleftrightarrow |1\rangle$ affect *all* the probability amplitudes. This also suggests that quantum computers can be extremely efficient.

However, when we make measurements, N qubits only leads to N bits of information. Therefore, even though it is very efficient and quick, there is only a small amount of output.

Example 1: Consider $f : \mathbb{Z}^+ \to \mathbb{R}$ a periodic function that maps $x \in [0, 2^L - 1]$ (i.e. takes in an L bit integer). There is some X such that $f(x + X) = f(x)$ and we wish to find X.

In a classical computer, we would evaluate $f(x)$ for multiple values of x. In general, we would expect around 2^{L-1} calls in the routine.

However, in a quantum computer, we need L qubits to store values of x (i.e. in the. argument register) and L qubits to store the result of $f(x)$ in the function register. Through a series of bit flips, we can create the state

$$|x\rangle|0\cdots 0\rangle \tag{1.10}$$

where the first braket is the input and the second braket is the function register. Then suppose we have a **quantum operation** $\hat{U}_f$ defined such that

$$\hat{U}_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle. \tag{1.11}$$

But if we prepare the initial state of the register not in x, but in a superposition (achieved via a **Hadamard gate**), then we can write:

$$\hat{U}_f \frac{1}{N}\left(\sum_{x=0}^{2^k-1}|x\rangle\right)|0\rangle = \frac{1}{N}\underbrace{\sum_{x=0}^{2^k-1}|x\rangle|f(x)\rangle}_{\text{massively entangled state}} \quad . \tag{1.12}$$

The difference is that all values of $f(x)$ are generated by a single call on $\hat{U}_f$. If we now apply something called the **Quantum Fourier Transform**

$$\hat{U}_{QFT}\sum_x |x\rangle|f(x)\rangle = \frac{1}{N}\sum_x |x\rangle|\tilde{f}(x)\rangle, \tag{1.13}$$

where $\tilde{f}$ is the **fourier transform,** which you will get a discrete graph of vertical bars separated a distance by $\frac{n}{X}$. If we do this a few times, we can extract what X is.

Quantum computers allow us in principle to evaluate periods very efficient. This is a very important problem in **number theory** since period finding helps a great deal in factoring.

Consider coprime n, a and define

$$f(x) = a^x \text{ mod } n. \tag{1.14}$$

This is a periodic function with period r. If we can figure out what r is, then

$$\gcd(a^{r/2} \pm 1, n) \tag{1.15}$$

is a factor of n. This is known as **Shor's Algorithm.**

1.3 Quantum Mechanics of Quantum Computers

Suppose there are three qubits. Recall that there are $2^3 = 8$ possible configurations. These form a basis for a 8-dimensional vector space. These basis states are known as a **computational basis**.

For a single basis $|\Psi\rangle = \alpha|0\rangle + \beta 1\rangle$, where α, β are complex probability amplitudes, then we have

$$|\alpha|^2 + |\beta|^2 = 1 \iff (\alpha^*, \beta^*)\begin{pmatrix}\alpha \\ \beta\end{pmatrix} = 1. \tag{1.16}$$

Now suppose we apply a transformation (i.e. operators and gates):

$$\begin{aligned}|\Psi\rangle &\mapsto |\Psi'\rangle \\ \alpha &\mapsto \alpha' \\ \beta &\mapsto \beta'.\end{aligned}$$

We can assume linearity (which has been experimentally validated), and therefore

$$\begin{aligned}\alpha' &= u_{00}\alpha + u_{01}\beta \\ \beta' &= u_{10}\alpha + u_{11}\beta\end{aligned}$$

which can be written as a matrix

$$\begin{pmatrix}\alpha' \\ \beta'\end{pmatrix} = \begin{pmatrix}u_{00} & u_{01} \\ u_{10} & u_{11}\end{pmatrix}\begin{pmatrix}\alpha \\ \beta\end{pmatrix} \iff |\Psi'\rangle = \hat{U}|\Psi\rangle. \tag{1.17}$$

And the complex conjugates are

$$(\alpha'^*, \beta'^*) = (\alpha^*, \beta^*)\begin{pmatrix}u_{00}^* & u_{10}^* \\ u_{01}^* & u_{11}^*\end{pmatrix} \iff \langle\Psi'| = \langle\Psi|\hat{U}^\dagger. \tag{1.18}$$

Here are some properties of the complex conjugate:

- $(\hat{A}\hat{B})^\dagger = \hat{B}^\dagger\hat{A}^\dagger$
- $\langle\psi'|\psi'\rangle = \langle\psi|\hat{U}^\dagger\hat{U}|\Psi\rangle = 1 \iff \hat{U}$ is unitary, which is true for all valid quantum operations on a closed system.

Let's look at some example gates:

- Bit-flip gate:

$$\hat{X} = \begin{pmatrix}0 & 1 \\ 1 & 0.\end{pmatrix} \tag{1.19}$$

  along with the rest of the Pauli matrices:

$$\hat{Y} = \begin{pmatrix}0 & -i \\ i & 0.\end{pmatrix} \tag{1.20}$$

$$\hat{Z} = \begin{pmatrix}1 & 0 \\ 0 & -1.\end{pmatrix} \tag{1.21}$$

$$\hat{I} = \begin{pmatrix}1 & 0 \\ 0 & 1.\end{pmatrix}. \tag{1.22}$$

- Phase-flip gate: $\hat{Z}$. Note that the overall **phase**, or "global" phase is irrelevant, since the norm of the probabilities stay the same.

2 Unitary Operators

2.1 SU(2)

An arbitrary 2×2 unitary is a matrix $\begin{pmatrix}a & b \\ c & d\end{pmatrix}$ such that $|ad - bc|^2 = 1$. In general, $ad - bc = e^{i\phi} \neq 1$. However in quantum computing, we don't typically care about the **phase** of our qubits, so without loss of generality, we can assume that $ad - bc = 1$. These are known as **special unitary matrices with dimension 2, or $SU(2)$.** We can therefore write it as

$$\hat{U} = \begin{pmatrix}a & b \\ -b^* & a^*\end{pmatrix}.$$

Any unitary matrix can be written as a linear combination of $\hat{I}, \hat{X}, \hat{Y}, \hat{Z}$.. Particularly,

$$\hat{U} = \begin{pmatrix}a_1 + ia_2 & b_1 + ib_2 \\ -b_1 + ib_2 & a_1 - ia_2\end{pmatrix} = a_1\hat{I} + ib_2\hat{X} + ib_1\hat{Y} + ia_2\hat{Z}. \tag{2.1}$$

Note that

$$1 = a_1^2 + a_2^2 + b_1^2 + b_2^2 \tag{2.2}$$

$$a_1 = \cos\theta \tag{2.3}$$

$$\{b_2, b_1, a_2\} = \sin\theta\{n_x, n_y, n_z\}. \tag{2.4}$$

We can thus express $\hat{U} = \cos\theta\hat{I} + i\sin\theta\boldsymbol{n}\cdot\boldsymbol{\sigma}$

2.2 Basis Change

We can introduce new bases use unitaries. Namely, $\hat{U}\,|0\rangle = |u\rangle\,, \hat{U}\,|1\rangle = |u_\perp\rangle$ are new basis vectors. These two will still be orthogonal.

2.3 Time Evolution

Suppose we have an evolving unitary

$$|\Psi(t)\rangle = \hat{U}(t)\,|\Psi(0)\rangle\,. \tag{2.5}$$

Taking the partial time derivative, and substituting in the above identity for $|\Psi(0)\rangle$, we have:

$$\begin{aligned}\frac{\partial}{\partial t}|\Psi(t)\rangle &= \frac{\partial \hat{U}(t)}{\partial t}|\Psi(0)\rangle \\ &= \left\{\frac{\partial \hat{U}(t)}{\partial t}\hat{U}^\dagger(t)\right\}|\Psi(t)\rangle\,.\end{aligned}$$

We can apply the product rule and the identity $(AB)^\dagger = B^\dagger A^\dagger$ to obtain

$$\begin{aligned}\hat{U}\hat{U}^\dagger &= I \\ \frac{\partial \hat{U}}{\partial t}\hat{U}^\dagger + \hat{U}\frac{\partial \hat{U}^\dagger}{\partial t} &= 0 \\ \frac{\partial \hat{U}}{\partial t}\hat{U}^\dagger &= -\left(\frac{\partial \hat{U}}{\partial t}\hat{U}^\dagger\right)^\dagger,\end{aligned}$$

which is an **anti-hermitian operator.** We can relate it to a hermitian operator $\hat{H}$.

$$\frac{\partial \hat{U}}{\partial t}\hat{U}^\dagger = \frac{\hat{H}}{i\hbar}, \tag{2.6}$$

where $\hat{H}$ is the **Hamiltonian**. Altogether, we end up with **Schrodinger's Equation:**

$$i\hbar\frac{\partial}{\partial t}|\Psi(t)\rangle = \hat{H}\,|\Psi(t)\rangle\,. \tag{2.7}$$

Usually we choose $\{|0\rangle, |1\rangle\}$ as the eigenstates of the Hamiltonian.

2.4 Measurements and Non-Unitary Operations

> If the particle is in a state $|\Psi\rangle$, measure of the variable $\hat{\Omega}$ will yield one of the eigenvalues of Ω with probability $P(\omega) = |\langle\omega|\Psi\rangle|^2$. The state of the system will change from $|\Psi\rangle$ to $|\omega\rangle$ as a result. - Shankar

For a qubit with the measurement operator $\hat{\Omega} = \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$ (with eigenvalues $\omega = 0, 1$), then $P(0) = |\alpha|^2$ and $P(1) = |\beta|^2$. The state at the end is equal to

$$|\Psi^{\text{after}}| = \frac{\hat{\Pi}_0\,|\Psi\rangle}{\sqrt{P(0)}} \text{ or } \frac{\hat{\Pi}_1\,|\Psi\rangle}{\sqrt{P(1)}} \tag{2.8}$$

where $\hat{\Pi}_0 = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$ and $\hat{\Pi}_1 = \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$ are rank-1 projectors, i.e. $\hat{\Pi}_0^2 = \hat{\Pi}$.

3 Two Qubit State

Recall that a two qubit state is written as

$$|\Psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle. \tag{3.1}$$

An **independent** or **separable** state can be written as a tensor product

$$|\Psi_{\text{sep}}\rangle = (a|0\rangle + b|1\rangle)_A \otimes (c|0\rangle + d|1\rangle)_B = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle. \tag{3.2}$$

Note that $\alpha\delta - \beta\gamma = acbd - adbc = 0$. We can immediately determine if a system can be separated by computing the **concurrence**

$$C = 2|\alpha\delta - \beta\gamma|. \tag{3.3}$$

If $C \neq 0$, then the system is not separable and is known as **entangled.**

3.1 Schmidt Decomposition Theorem

Theorem: Any two-qubit pure state can be written as

$$|\Psi\rangle = \hat{U}_A \otimes \hat{U}_B (\lambda_0|00\rangle + \lambda_1 11), \tag{3.4}$$

where λ_0, λ_1 are real, positive constants known as **singular values** and they satisfy $\lambda_0^2 + \lambda_1^2 = 1$. The operators $\hat{U}_A, \hat{U}_B$ are unitaries applied separately to each qubit.

Consider the unitary operators $\hat{U}_A = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix}$ and $\hat{U}_B = \begin{pmatrix} c & d \\ -d^* & c^* \end{pmatrix}$. Therefore,

$$\begin{aligned} |\Psi\rangle &= \lambda_0 (a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle) + \lambda_1(-b^*|0\rangle + a^*|1\rangle)(-d^*|0\rangle + c^*|1\rangle) && (3.5)\\ &= (\lambda_0 ac + \lambda_1 b^* d^*)|00\rangle + (\lambda_0 ad - \lambda_1 b^* c^*)|01\rangle + (\lambda_0 bc - \lambda_1 a^* d^*)|10\rangle + (\lambda_0 bd + \lambda_1 a^* c^*)|11\rangle. && (3.6)\end{aligned}$$

This looks very messy, but we can compute the concurrence (and after a length but straightforward computations), we get

$$C = 2\lambda_0\lambda_1. \tag{3.7}$$

Using $\lambda_0^2 + \lambda_1^2 = 1$, we can obtain the quadratic equation

$$\lambda^4 - \lambda^2 + (C/2)^2 = 0, \tag{3.8}$$

so λ_0, λ_1 are determined by C. The maximum value of C is $C_{\text{max}} = 1$, which occurs at $\lambda_{\text{crit}} = \frac{1}{\sqrt{2}}$. At $C = 1$, it is known as a **maximally entangled state.**

This isn't justified yet, but C is the measure of entanglement for 2-qubit states.

Proof. Let us rewrite

$$|\Psi\rangle = \sum_{i,j=0}^{1} \chi_{ij}|i\rangle|j\rangle \tag{3.9}$$

where χ_{ij} are elements of a 2×2 matrix $\chi = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Note that χ is not hermitian, but both $\hat{\chi}\hat{\chi}^\dagger$ and $\hat{\chi}^\dagger\hat{\chi}$ are hermitian and their eigenvalues are positive.

We can show they are hermitian by a direct computation. To show their eigenvalues are positive, note that $\langle\phi|\phi\rangle \geq 0$ for any state ϕ and we can write:

$$\langle\phi|\hat{\chi}\hat{\chi}^\dagger|\phi\rangle = \langle\phi'|\phi'\rangle \geq 0. \tag{3.10}$$

Note that $|\phi'\rangle$ is an eigenvector of $\hat{\chi}\hat{\chi}^\dagger$. Then all the eigenvalues are positive.

Consider an aribtrary matrix $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$. The determinant can be determined by $\lambda^2 - (\text{Tr})\lambda + (\text{Det}) = 0$. The trace of $\hat{\chi}\hat{\chi}^\dagger$ is 1 and the determinant is $C^2/4$. This allows us to calculate λ_0, λ_1. Define

$$\Lambda = \begin{pmatrix} \lambda_0 & 0 \\ 0 & \lambda_1 \end{pmatrix}. \tag{3.11}$$

This allows us to write

$$\hat{\chi}\hat{\chi}^\dagger = \hat{U}\Lambda^2\hat{U}^\dagger$$
$$\hat{\chi}^\dagger\hat{\chi} = \hat{V}\Lambda^2\hat{V}^\dagger.$$

Combining the two together, we end up with the **singular value decomposition**

$$\hat{\chi} = \hat{U}\hat{\Lambda}\hat{V}^\dagger. \tag{3.12}$$

We can write an expression for each entry:

$$\chi_{ij} = \sum_{p=0}^{1} U_{ip}\lambda_p V_{jp}^*, \tag{3.13}$$

which directly leads to the desired relationship. □

3.2 Operations on Two Qubits

There are various ways to perform operations. Here are a few ways:

1. **Local Unitaries** apply to only one qubit. Namely,

$$|\Psi'\rangle = (\hat{U}\otimes\hat{I})\,|\Psi\rangle\,. \tag{3.14}$$

If $\hat{U} = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix}$, then this operation can be represented by

$$\begin{pmatrix} \alpha' \\ \beta' \\ \gamma' \\ \delta' \end{pmatrix} = \begin{pmatrix} a & 0 & b & 0 \\ 0 & a & 0 & b \\ -b^* & 0 & a^* & 0 \\ 0 & -b^* & 0 & a^* \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} a\hat{I} & b\hat{I} \\ -b^*\hat{I} & a^*\hat{I} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = (\hat{U}\otimes\hat{I}) \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}. \tag{3.15}$$

A similar relationship can be found for operations in the form $\hat{I}\otimes\hat{V}$.

It is important to recognize that local operations can never increase entanglement. So how can we increase entanglement? We start with two qubits in $|0\rangle\,|0\rangle$, and apply a unitary $\hat{U}_1 = \lambda_0\hat{I} - i\lambda_1\hat{Y}$ to qubit 1,

$$|0\rangle \to \lambda_0\,|0\rangle + \lambda_1\,|1\rangle\,. \tag{3.16}$$

such that

$$|\Psi_1\rangle = \lambda_0\,|00\rangle + \lambda_1\,|11\rangle\,. \tag{3.17}$$

We then apply a **CNOT** gate by applying a bit flip to qubit 2 if qubit 1 is in $|1\rangle$ and do nothing if qubit 1 is in $|0\rangle$. However, we have to do this unitarily and reversibly. We can write:

$$\text{CNOT} = \hat{\Pi}_0\otimes\hat{I} + \hat{\Pi}_1\otimes\hat{X}. \tag{3.18}$$

so

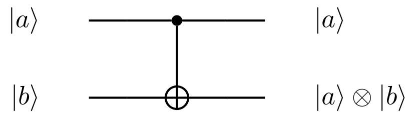
$$|\Psi_2\rangle = \text{CNOT}(\Psi_1) = \lambda_0\,|00\rangle + \lambda_1\,|11\rangle\,. \tag{3.19}$$

We then apply local unitaries $\hat{U}_a$ and $\hat{U}_b$, so

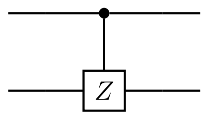
$$|\Psi\rangle_3 = (\hat{U}_a\otimes\hat{U}_b)(\lambda_0\,|00\rangle + \lambda_1\,|11\rangle). \tag{3.20}$$

4 Universal Two-Qubit Gates

A **universal 2-qubit gate** (such as the CNOT gate), along with local unitary operators, can be used to create any two-qubit system. A CNOT gate can be represented as



To test if other gates are universal, we can see if it can be transformed into a CNOT gate. For example, the control-Z gate,



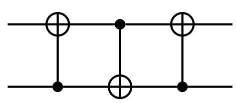
is also universal. This is equivalent since $HZH = X$. This is represented by the **control-Z** matrix, given by

$$\hat{U}_{CZ} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \tag{4.1}$$

The **SWAP** gate is given by

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{4.2}$$

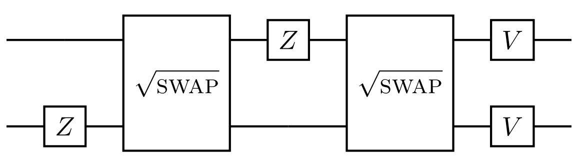
and reverses the roles of the two qubits, which is equivalent to the circuit


.

Note that the SWAP gate is not universal. However, the **ROOT-SWAP** gate is universal and is given by:

$$\sqrt{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & (1+i)/2 & (1-i)/2 & 0 \\ 0 & (i-1)/2 & (1+i)/2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{4.3}$$

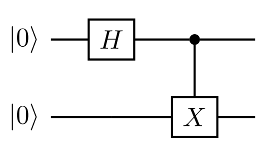
We can use the SWAP gate along with local unitaries to create control-Z via the following:



where $V = \sqrt{Z} = (\hat{I} - i\hat{Z})/\sqrt{2}$, and can be checked by matrix multiplication.

4.1 Maximally Entangled States

Recall that a state is maximally entangled if and only if $C = 2|\alpha\delta - \beta\gamma| = 1$. Let us see how we can construct such a state. Consider the circuit:



So, the qubits gets transformed to:

$$|00\rangle \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi_+\rangle\,, \tag{4.4}$$

so the concurrence is 1. It turns out we can construct more maximally entangled states. Namely,

$$|\beta_k\rangle = i(\hat{I} \otimes \hat{\sigma}_k)\,|\beta\rangle\,. \tag{4.5}$$