ESILV LÉONARD DE VINCI | ÉCOLE D'INGÉNIEURS PARIS-LA DÉFENSE

Quantum Computing

[Summary]

PANSERA Tony

November 5, 2025

Contents

1 Unit 1: Quantum Information

1.1 Single systems

1.1.1 Classical information

First, we will introduce the idea of classical information, as it brings several key points similar to how quantum information works.

Let's consider a physical system that stores information, called X, and let's assume X can be one of a finite number of **classical states**. Let's denote this classical state set by Σ.

Examples:

- If X is a bit, then $\Sigma = \{0, 1\}$
- If X is a dice, then $\Sigma = \{0, 1, 2, 3, 4, 5, 6\}$

There may be an **uncertainty** about the classical state of the system, where each classical state has some **probability** associated with it. We can make an analogy with probability, where X is a random variable and Σ the support.

For example, if X is a bit, then perhaps we can have this **probabilistic state** of X:

$$P(X = 0) = \frac{3}{4} \text{ and } P(X = 1) = \frac{1}{4}$$

This probabilistic state can also be represented by a **column vector**:

$$\begin{pmatrix} \frac{3}{4} \\ \frac{1}{4} \end{pmatrix} \quad \begin{matrix} \text{<- entry corresponding to 1} \\ \text{<- entry corresponding to 0} \end{matrix}$$

This vector is called a **probability vector**, where all entries and non-negative real numbers and the sum of all entries is 1.

1.1.2 Dirac notation (part 1)

Definition: Let Σ be any classical state set, and assume the elements of Σ have been ordered. We denote by $|a\rangle$ the column vector having 1 in the entry corresponding to $a \in \Sigma$, with 0 for all other entries.

For example, for the binary alphabet ($\Sigma = \{0, 1\}$), we have:

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

Vectors of this form are called **standard basis vectors**, every vector can be expressed uniquely as a linear combination of standard basis vectors.

With the previous example we have:

$$\begin{pmatrix} \frac{3}{4} \\ \frac{1}{4} \end{pmatrix} = \frac{3}{4}|0\rangle + \frac{1}{4}|1\rangle$$

Definition of bra: Let Σ be any classical state set, and assume the elements of Σ have been ordered. We denote by $\langle a|$ the column vector having 1 in the entry corresponding to $a \in \Sigma$, with 0 for all other entries.

For example, for the binary alphabet, we have:

$$\langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix} \quad \text{and} \quad \langle 1| = \begin{pmatrix} 0 & 1 \end{pmatrix}$$

Multiplying a row vector to a column vector yields to a scalar. We write:

$$\langle a|b\rangle = \langle a|\,|b\rangle$$

1.1.3 Measuring probabilistic states

If we **measure** a system X while it is in some probabilistic state, we can see a **classical state** chosen at random according to the probabilities.

Suppose we see the classical state $a \in \Sigma$. From our point of view, it changes the probabilistic state of X as we have recognized that $X = a$. Now we have:

$$P(X = a) = 1$$

This probabilistic state is represented by the vector $|a\rangle$.

We can think of it as a transition of knowledge as opposed to a physical transition.

One final note is that to another person who didn't see that the state was when we measured it, the probabilistic state wouldn't change as a result

of us having measured it. And that's okay because different individuals can have different knowledge about a system.

1.1.4 Deterministic operations

Definition: Every function $f : \Sigma \to \Sigma$ describes a **deterministic operation** that transforms the classical state a into $f(a)$.

Given any function $f : \Sigma \to \Sigma$, there is a unique matrix M satisfying:

$$M\,|a\rangle = |f(a)\rangle$$

This matrix has exactly one 1 in each column, and 0 for all other entries:

$$M_{b,a} = \begin{cases} 1 & \text{if } b = f(a), \\ 0 & \text{if } b \neq f(a) \end{cases}$$

The action of a deterministic operation is described by **matrix-vector multiplication**:

$$v \longmapsto Mv$$

This matrix may be expressed as:

$$M = \sum_{b \in \Sigma} |f(b)\rangle \langle b|$$

Demonstration: As we can see, we have:

$$M\,|a\rangle = \left(\sum_{b \in \Sigma} |f(b)\rangle \langle b| \right) |a\rangle$$

Thanks to the linearity of matrices, we can remove the parenthesis. Moreover, matrix-vector multiplication is associative, so we can group $\langle b|$ and $|a\rangle$. We have:

$$\left(\sum_{b \in \Sigma} |f(b)\rangle \langle b| \right) |a\rangle = \sum_{b \in \Sigma} |f(b)\rangle \langle b|a\rangle$$

Now, as a is fixed, and as we sum over all the possible choices of b, $\langle b|a\rangle$ is always going to be equal to zero when b is not equal to a. When $b = a$, we finally have:

$$M\,|a\rangle = \sum_{b \in \Sigma} |f(b)\rangle \langle b|a\rangle = |f(a)\rangle$$

1.1.5 Probabilistic operations

Definition: Probabilistic operations are classical operations that may introduce randomness or uncertainty.

Example: Here is a probabilistic operation on a bit:

- If the classical state is 0, then do nothing
- If the classical state is 1, the flip the bit with probability 1/2.

Probabilistic operations can also be represented by matrices, called stochastic matrices:

- All entries are nonnegative real numbers
- The entries in every column sum to 1

In other words, every column forms a probability vector. When you apply it to a vector, or a classical state, it tells you what the probabilistic state is (we still don't know, the probabilistic state depends on the classical state) that comes out as a probability vector.

In our previous example, we have the matrix:

$$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix}$$

We can also think of probabilistic operations in a different way, as random choices of deterministic operations.

For instance, in our example, we can write:

$$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

This is always possible, for every probabilistic operation.

1.1.6 Composing operations

Suppose X is a system and M_1, M_2 are stochastic matrices representing probabilistic operations on X. Applying the first, then second probabilistic operation to the vector v, we can write:

$$M_2(M_1 v) = (M_2 M_1)v$$

As matrices are commutative. The probabilistic operation obtained by composing the first and second probabilistic operations is then represented by the matrix product $M_2 M_1$.

1.1.7 Quantum information

Now that we have introduced what is classical information and how it works, we can start talking about quantum information. It works in a very similar way to classical information with some key differences.

Definition: A quantum state of a system is represented by a column vector whose indices are placed in correspondence with the classical states of that system:

- The entries are complex numbers
- The sum of the absolute values squared of the entries must equal 1

Reminder: The euclidean norm for vectors with complex entries is defined like this:

$$v = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \Longrightarrow \|v\| = \sqrt{\sum_{k=1}^{n} |\alpha_k|^2}$$

Quantum state vectors are therefore **unit vectors** with respect to this norm.

Examples of qubit states:

- Standard basis stated: $|0\rangle$ and $|1\rangle$
- Plus/minus states:

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \text{ and } |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

- A state without a special name:

$$\frac{1+2i}{3}|0\rangle - \frac{2}{3}|1\rangle$$

1.1.8 Dirac notation (part 2)

In quantum mechanics, the *ket* notation is used to represent a quantum state of a particle. A ket, written as $|\psi\rangle$, is a **vector in a complex**

Hilbert space that fully describes the system's state. It is usually **normalized**, meaning its inner product with itself equals one ($\langle\psi|\psi\rangle = 1$), which ensures that the total probability of finding the particle in any possible state is 1 (this is the same as saying that its norm is equal to 1, as explained in the previous section).

Kets are typically used to represent **pure states**, where the system is in a well-defined condition: they can be expressed as **linear combinations** (or superpositions) of basis states, such as $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$, where a and b are complex probability amplitudes satisfying $|a|^2 + |b|^2 = 1$. As we can see, we have:

$$\langle\psi|\psi\rangle = |a|^2 + |b|^2 = 1 = \sqrt{|a|^2 + |b|^2} = \|\psi\|$$

The dirac notation can be used for arbitrary vectors: any name can be used in place of a classical state. Kets are column vectors, bras are row vectors.

For any column vector $|\Psi\rangle$, the row vector $\langle\Psi|$ is the **conjugate transpose** of $|\Psi\rangle$:

$$\langle\Psi| = |\Psi\rangle^\dagger$$

Example: The notation $|\Psi\rangle$ is commonly used to refer to an arbitrary vector:

$$|\Psi\rangle = \frac{1+2i}{3}\,|0\rangle - \frac{2}{3}\,|1\rangle$$

$$\langle\Psi| = \frac{1-2i}{3}\,\langle 0| - \frac{2}{3}\,\langle 1|$$

1.1.9 Measuring quantum states

When we look at a system when it's in a quantum state, we don't see a quantum state, just like we don't see probabilistic states. We see classical states. If we want to know something about a quantum system, we have to measure it to extract information.

In this part we will focus first on **Standard basis measurements**:

- The possible outcomes are the classical states
- The probability for each classical state to be the outcome is the **absolute value squared** of the corresponding quantum state vector entry

As we have seen before, the euclidean norm of a quantum state vector must equal 1. As such, every absolute squared value can be represented as the probability of the system being in that state.

For example, measuring the quantum state

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

yields an outcome as follows:

$$P(\text{outome is } 0) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} \quad P(\text{outome is } 1) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

Just like we've seen in the probabilistic setting, if we measure a system when it is in a quantum state, the state will change as a result of having performed the measurement. In other words, measuring a system changes its quantum state: if we obtain the classical state a, the new quantum state becomes $|a\rangle$.

This phenomenon is often referred as a collapse of the quantum state. Notice that is we measure the system a second time, we would get exactly the same result of the first measurement, there is a limit of how much information can be extracted from a quantum state.

1.1.10 Unitary operations

The set of allowable **operations** that can be performed on a quantum state is different than it is for classical information. Operations on quantum state vectors are represented by **unitary matrices**.

Definition: A square matrix $U \in \mathcal{M}_n(\mathbb{C})$ is unitary if it satisfies the equalities:

$$U^\dagger U = \mathbf{1} = UU^\dagger$$

where $U^\dagger$ is the conjugate transpose of U and $\mathbf{1}$ the identity matrix.

The condition that an $n \times n$ matrix U is unitary is equivalent to

$$\|Uv\| = \|v\|$$

for every n-dimensional column vector v with complex number entries.

If v is a quantum state vector, then Uv is also a quantum state vector as $\|Uv\| = \|v\| = 1$.

This is the same we had with stochastic matrices and probability vectors, stochastic matrices always transform probability vectors into probability vectors.

1.1.11 Qubit unitary operations

We will present some popular Qubit unitary operations.

1. **Pauli operations:** Pauli operations are ones represented by the Pauli matrices:

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_{\mathbf{x}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_{\mathbf{y}} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_{\mathbf{z}} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

   These particular matrices happen to be equal to their own conjugate transposes, they are all Hermitian matrices.

   The operation σ_X is also called a **bit flip** (NOT operation) and the σ_z operation is called a **phase flip**:

$$\sigma_x |0\rangle = |1\rangle \quad \sigma_z |0\rangle = |0\rangle$$
$$\sigma_x |1\rangle = |0\rangle \quad \sigma_z |1\rangle = -|1\rangle$$

2. **Hadamard operation:** The Hadamard operation is represented by this matrix:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

   The Hadamard gate introduces state superposition. If we apply this gate to $|0\rangle$ and $|1\rangle$ we have:

$$H |0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle$$
$$H |1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle$$

   On the other hand, if we perform the Hadamard operation of $|+\rangle$ and $|-\rangle$ respectively, we can find back $|0\rangle$ and $|1\rangle$:

$$H |+\rangle = |0\rangle$$
$$H |-\rangle = |1\rangle$$

3. **Phase operations:** A phase operation is one described by the matrix:

$$P_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

for any choice of a real number θ.

Note: Thanks to the linearity of matrices, we can do unitary operations only using the Dirac notation.

For example: Let $T = P_{\pi/4}$, we have $T|0\rangle = |0\rangle$ and $T|1\rangle = e^{i\frac{\pi}{4}}|1\rangle = \frac{1+i}{\sqrt{2}}|1\rangle$.
Let's compute $HT|+\rangle$:

$$\begin{aligned}
HT|+\rangle &= HT\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \\
&= H\left(\frac{1}{\sqrt{2}}T|0\rangle + \frac{1}{\sqrt{2}}T|1\rangle\right) \\
&= H\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1+i}{2}|1\rangle\right) \\
&= \frac{1}{\sqrt{2}}H|0\rangle + \frac{1+i}{2}H|1\rangle \\
&= \frac{1}{\sqrt{2}}|+\rangle + \frac{1+i}{2}|-\rangle \\
&= \left(\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle\right) + \left(\frac{1+i}{2\sqrt{2}}|0\rangle - \frac{1+i}{2\sqrt{2}}|1\rangle\right) \\
&= \left(\frac{1}{2} + \frac{1+i}{2\sqrt{2}}\right)|0\rangle + \left(\frac{1}{2} - \frac{1+i}{2\sqrt{2}}\right)|1\rangle
\end{aligned}$$

1.1.12 Composing unitary operations

Compositions of unitary operations are represented by **matrix multiplication**. Similar to the probabilistic setting with stochastic matrices, the matrix for the first performed operation must appear on the right-hand side of the matrix product and the last one on the left-hand side.

Coming back to the previous σ_x operation, is important to see it as a rotation and not a boolean inversion. We can find a squareroot of σ_x and apply it twice:

$$\sqrt{\sigma_x} = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} \text{ and we have } \sqrt{\sigma_x} \times \sqrt{\sigma_x} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x$$

This example reveals that quantum operations behave very differently from classical operations. There is no classical operation that gives us a NOT operation if we perform it twice.

1.2 Multiple systems

Now that we've described how single systems work, we'll explain how multiple systems work.

1.2.1 Classical states

Suppose $X_1, ..., X : n$ are systems having classical state sets $\Sigma_1, ..., \Sigma_n$ respectively.

The classical state set of the n-tuple $(X_1, ..., X_n)$, viewed as a single compound system, is the Cartesian product

$$\Sigma_1 \times ... \times \Sigma_n = \{(a_1, ..., a_n) : a_1 \in \Sigma_1, ..., a_n \in \Sigma_n\}$$

An n-tuple $(a_1, ..., a_n)$ may also be writen as a **string** $a_1...a_n$.

Example: If $\Sigma_1 = \Sigma_2 = \Sigma_3 = \{0, 1\}$, then the classical state set of (X_1, X_2, X_3) is:

$$\Sigma_1 \times \Sigma_2 \times \Sigma_3 = \{(0,0,0), (0,0,1), (0,1,0), (0,1,1),$$
$$(1,0,0), (1,0,1), (1,1,0), (1,1,1)\}$$

Written as strings, the classical states look like this: 000,001,010,011,100,101,110,111

Convention: Cartesian products of classical state sets are ordered **lexicographically**:

- We assume the individual classical state sets are already ordered
- Significance decreases from left to right

Example: The cartesian product $\{1, 2, 3\} \times \{0, 1\}$ is ordered like this:

$$(1,0), (1,1), (2,0), (2,1), (3,0), (3,1)$$

This is the same as how it works with natural numbers. We first look at the first number, and if they are equal we look at the second etc.

1.2.2 Probabilistic states

Probabilistic states of compound systems associate probabilities with the Cartesian product of the classical state sets of the individual systems.

Example: This is a probabilistic state of a pair of bits (X, Y):

$$P((X,Y) = (0,0)) = \frac{1}{16}$$
$$P((X,Y) = (0,1)) = \frac{1}{12}$$
$$P((X,Y) = (1,0)) = \frac{1}{2}$$
$$P((X,Y) = (1,1)) = \frac{1}{4}$$

Definition: For a given probabilitic state of (X, Y), we say that X and Y are **independent** if, $\forall a \in \Sigma, \forall b \in \Gamma$:

$$P((X,Y) = (a,b)) = P(X = a)P(Y = b)$$

If (X, Y) is expressed as a vector, it is expressed like this:

$$|\pi\rangle = \sum_{(a,b)\in\Sigma\times\Gamma} p_{ab} |ab\rangle$$

The systems X and Y are independent if there exist probability vectors

$$|\Phi\rangle = \sum_{a\in\Sigma} q_a |a\rangle \quad \text{and} \quad |\Psi\rangle = \sum_{b\in\Gamma} r_b |b\rangle$$

such that $p_{ab} = q_a r_b$, for all $a \in \Sigma$ and $b \in \Gamma$. It is essentially a rephrasing of the original definition, but applied to vectors.

In the case that X and Y are not independent, they are correlated.

If we take our previous example, we can write the probabilistic state of the pair of bits (X, Y) as:

$$|\pi\rangle = \frac{1}{6}|00\rangle + \frac{1}{12}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{4}|11\rangle$$

We can see that X and Y are independent as we can have those two

probability vectors that satisfy the independance requirements:

$$|\Phi\rangle = \frac{1}{4}|0\rangle + \frac{3}{4}|1\rangle \quad \text{and} \quad |\Psi\rangle = \frac{2}{3}|0\rangle + \frac{1}{3}|1\rangle$$

1.2.3 Tensor products of vectors

Definition: The **tensor product** of two vectors

$$|\Phi\rangle = \sum_{a\in\Sigma} \alpha_a |a\rangle \quad \text{and} \quad |\Psi\rangle = \sum_{b\in\Gamma} \beta_b |b\rangle$$

is the vector

$$|\Phi\rangle \otimes |\Psi\rangle = \sum_{(a,b)\in\Sigma\times\Gamma} \alpha_a\beta_b |ab\rangle$$

Equivalently, the vector $|\pi\rangle = |\Phi\rangle \otimes |\Psi\rangle$ is defined by this condition:

$$\langle ab|\pi\rangle = \langle a|\Phi\rangle \langle b|\Psi\rangle \quad \text{for all } a \in \Sigma \text{ and } b \in \Gamma$$