1 Quantum Mechanics Model

[SECTION IN PROGRESS]

1.1 Bra-ket notation and linear algebra preamble

Let the qubit as a rigorous mathematical construction. As we have already mentioned, a single qubit will be a vector in a complex vector space, but we will need that space to have some extra properties. That is, it will be a projective Hilbert space. Let us review the necessary linear algebra.

Let V be a complex vector space. That is, a vector space over $\mathbb{C}$. We will restrict our study to finite complex vector spaces. If z is a vector in V, we will denote its coordinates either as $z = (z_1, z_2, \dots, z_n)$ or by column notation:

$$z = \begin{pmatrix} z_1 \\ z_2 \\ \dots \\ z_n \end{pmatrix}$$

Since V is a vector space we have two basic operations: (vector) addition and scalar multiplication.

In quantum mechanics, the usual notation is the Dirac's, also know *bra-ket* notation. In this context, vectors in a complex vector space are denoted as $|\varphi\rangle$ and are known as *kets*. The only exception to this is the zero vector, which will be denoted as $0 = (0, \dots, 0)$ instead of $|0\rangle$ since $|0\rangle$ will be used as something completely different. A *vector subspace* W of V is a subset of W closed for addition and scalar multiplication.

A *base* of a vector space is a set of vectors $|v_1\rangle, \dots, |v_n\rangle$ such that they are linearly independent and any given vector $|v\rangle$ can be written as a linear combination of them: $|v\rangle = \sum_{i=1}^{n} \alpha_i |v_i\rangle$. The *dimension* of a vector space is the number of elements in any of its bases, which is independent from the chosen base.

1.1.1 Linear operators

Definition 1. Given two complex vector spaces V and W, a *linear operator* is an application $M : V \to W$ that is linear in its inputs:

$$M\Big(\alpha|u\rangle + \beta|w\rangle\Big) = \alpha M(|u\rangle) + \beta M(|w\rangle)$$

If V to W have dimensions n and m respectively, there is a bijection between the operators from V to W and the n by m matrices. Given an operator M, the obtained matrix M' is called the *matrix representation* of the linear operator. Furthermore, $M(|u\rangle) = M' \cdot |u\rangle$, so we usually denote the linear operator and its matrix representation by the same letter, and $M(|u\rangle)$ simply as $M|u\rangle$.

We will refer to linear operators simply as *operators*.

1.1.2 Inner product and Hilbert Spaces

Lets define another operation within the complex vector spaces.

Definition 2. Let V be a complex vector space. An inner product $\langle\cdot|\cdot\rangle : V^2 \to \mathbb{C}$ is a function such that:

1) $\langle\cdot|\cdot\rangle$ is sesquilinear. That is,

1.1) $\langle\cdot|\cdot\rangle$ is conjugate symmetric: for all u, v in V, $\langle u|v\rangle = \overline{\langle v|u\rangle}$.

1.2) $\langle\cdot|\cdot\rangle$ is linear on the second variable: for all u, v, w in V and α, β in $\mathbb{C}$:

$$\langle u|\alpha v + \beta w\rangle = \alpha\langle u|v\rangle + \beta\langle u|w\rangle$$

2) $\langle\cdot|\cdot\rangle$ is definite positive. That is, for all u in V, $\langle u|u\rangle \geq 0$ and $\langle u|u\rangle = 0 \iff v = 0$.

Given this properties it can easily be proven that $\langle\cdot|\cdot\rangle$ is also conjugate linear on the first variable. That is, for all u, v, w in V and α, β in $\mathbb{C}$:

$$\langle\alpha u + \beta v|w\rangle = \overline{\alpha}\langle u|w\rangle + \overline{\beta}\langle v|w\rangle$$

We will sometimes denote the inner product $\langle\cdot|\cdot\rangle$ as $(\cdot,\cdot)$ to simplify notation.

Two vectors are said to be *orthonormal* if there inner product is zero. We define the norm of a vector $|v\rangle$ by:

$$\| \, |v\rangle \, \| = \sqrt{\langle v|v\rangle}$$

A *unit vector* is a vector $|v\rangle$ such that $\| \, |v\rangle \quad \|= 0$. We also say that $|v\rangle$ is *normalized*, and we can normalize any vector except the zero vector by dividing it by its norm.

A base $|v_1\rangle, \ldots, |v_n\rangle$ is said to be *orthonormal* if every vector is a unit vector and they are pairwise orthogonal. That is, $\langle v_i|v_j\rangle = \delta_{ij}$ where

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

Definition 3. An *inner product space* is a vector space with an associated inner product. A **Hilbert Space** is an inner product space that is also complete. space.

Hausdorff's Theorem states that every finite normed space is complete [TODO: ref Payá], therefore every finite inner product space over $\mathbb{C}$ is a Hilbert space. Again, by Hausdorff's theorem we know that every n dimensional Hilbert space is isomorphic to $\mathbb{C}^n$. Thus, $\mathbb{C}^n$ is the canonical n dimensional Hilbert space and we will focus our study on these spaces.

The canonical inner product in $\mathbb{C}^n$ is:

$$\langle u|v\rangle \ = \sum_{i=1}^{n} \overline{u_i} v_j$$

where $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$, for every u, v in $\mathbb{C}^n$.

Let $\alpha = a + i \cdot b \in \mathbb{C}$. We define the *conjugate*, $\bar{\alpha}$, as $\bar{\alpha} = a - i \cdot b$.

1.1.3 Outer product

Definition 4. Definition: Let V, W be two vector spaces and $|v\rangle \in V, |w\rangle \in W$. We define the *outer product* between $|v\rangle$ and $|w\rangle$, $|w\rangle\langle v|$, as the only linear operator such that for any $|v'\rangle \in V$,

$$(|w\rangle\langle v|) \ |v'\rangle = |w\rangle\langle v|v'\rangle = \langle v|v'\rangle|w\rangle$$

This identities provide a dual interpretation: the already known product of a complex value $\langle v|v'\rangle$ with a vector $|w\rangle$, and the application of the new operator, the outer product $|w\rangle\langle v|$ to the vector $|v'\rangle$. The outer product is defined so that this duality is held.

Let us consider linear combinations of outer products. By definition, $\sum_i a_i|w_i\rangle\langle v_i|$ is the operator that transforms $|v'\rangle$ into $\sum_i a_i|w_i\rangle\langle v_i|v'\rangle = \sum_i a_i\langle v_i|v'\rangle|w_i\rangle$.

The most important result concerning outer products is the *completeness relation*:

Proposition 1 (Completeness relation)**.** *Let $|i\rangle$ be any orthonormal basis of a finite vector space V. Then:*

$$\sum_i |i\rangle\langle i| = I$$

Proof. Let $|v\rangle \in H$. $|v\rangle$ can be expressed as $\sum_i v_i|i\rangle$ for some complex numbers v_i. Notice that $\langle i|v\rangle = v_i$. Therefor:

$$|v\rangle = \sum_i v_i|i\rangle = \sum_i \langle i|v\rangle|i\rangle = \sum_i |i\rangle\langle i|v\rangle = \left(\sum_i |i\rangle\langle i|\right)|v\rangle$$

Since $|v\rangle$ was arbitrary, proves that $\sum_i |i\rangle\langle i| = I$. □

Corollario 1 (Cauchy-Schwarz inequality)**.**

Proof. TODO: To be copied, Box 2.1, page 68, Nielsencheng. □

1.1.4 Eigenvectors and eigenvalues

Definition 5. Let V be a vector space and A an operator on V. An *eigenvector* is a non zero vector $|v_\lambda\rangle$ such that $A|v_\lambda\rangle = \lambda|v_\lambda\rangle$ for a complex value λ called the associated *eigenvalue.*

Eigenvalues and associated eigenvectors will usually be denoted with the same letter for simplicity: λ and $|\lambda\rangle$. We assume the reader is familiar with eigenvectors and values basic notions. For instance, that they may be calculated using the *characteristic equation*: $|I - \lambda A| = 0$.

Definition 6. A *diagonal representation* of an operator A is a representation $\sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i|$ where the $|\lambda_i\rangle$ form an orthonormal set of A's eigenvectors and λ_i are the respective eigenvalues. An operator is said to be *diagonalizable* if it allows a diagonal representation.

Example 1. As an example of this, let us consider the following matrix:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

This matrix is called the *Z Pauli* matrix. It is relevant for quantum computing and it will be introduced later on along with the rest of the Pauli matrices. For now, lets compute its diagonalizable representation. Since it is already diagonal we can infer that its eigenvalues are $\{1, -1\}$. Computing the diagonal representation we realize that a pair orthonormal eigenvectors are $\{|0\rangle, |1\rangle\}$ respectively. Therefore:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

A characterization of diagonalizable operators is provided in Theorem (TODO: add reference to spectral decomposition theorem).

1.1.5 Adjoint and normal operators

Another way of looking at the inner product is the *adjoint*.

Definition 7. Let A be an operator between $\mathbb{C}^n$ and $\mathbb{C}^m$, finite dimensional Hilbert spaces. That is, $A \in \mathcal{M}_{n\times m}(\mathbb{C})$. Then, its *adjoint* or *conjugate transpose* $A^\dagger$ is defined by:

$$(A^\dagger)_{ij} = \bar{A}_{ji}$$

If $|v\rangle$ is a vector, we can compute its adjoint by seeing it as a matrix. By convention, we will denote $|v\rangle^\dagger = \langle v|$. Adjoints of vector are usually called *bras*, making given sense to the *bra-ket* notation since $\langle v| \cdot |v\rangle = \langle v|v\rangle$, where $\cdot$ denotes the dot product.

Some useful algebraic identities associated to adjoints are:

- Given an operator $A \in \mathcal{M}_n(\mathbb{C})$, $A^\dagger$ is the only operator such that for any two vectors $|u\rangle, |v\rangle \in \mathbb{C}^n$: $(|u\rangle, A|v\rangle) = (A^\dagger|u\rangle, |v\rangle)$
- For any two operators A, B, $(AB)^\dagger = B^\dagger A^\dagger$.
- As a corollary, for any vector $|v\rangle$ and for any operator A, $(A|v\rangle)^\dagger = \langle v|A^\dagger$.

Definition 8. An operator A is said to be *normal* if $AA^\dagger = A^\dagger A$.

Normal operators have significant relevancy thanks to the following result:

Theorem 1 (Spectral Decomposition Theorem)**.** *An operator A is normal if and only if it is diagonalizable.*

Proof. TODO: To be copied, Box 2.2, page 72, Nielsenchen. □

There are two particular cases of normal operators that will be of special interest for us:

Definition 9. An operator A is said to be *Hermitian* if its adjoint is itself: $A^\dagger = A$.

Definition 10. A matrix U is said to be *unitary* if $UU^\dagger = I$. Similarly, an operator is said to be *unitary* if $UU^\dagger = I$. A unitary operator U also fulfills that $U^\dagger U = I$.

Clearly, Hermitian and unitary operators are also normal.

Corollario 2. *Any Hermitian operator is diagonalizable. Any unitary operator is diagonalizable.*

The importance of unitary matrices and operators in quantum computing relies on the following

Proposition 2. *Unitary operators preserve inner product between vectors. Thus, they also preserve the norm of a vector.*

Proof. Let $|u\rangle, |v\rangle \in \mathbb{C}^n$ and $U \in \mathcal{M}_n(\mathbb{C})$ be a unitary operator. Then:

$$(U|u\rangle, U|v\rangle) = \langle u|U^\dagger U|v\rangle = \langle u|I|v\rangle = \langle u|v\rangle = (|u\rangle, |v\rangle)$$

Which proves the proposition. $\square$

1.1.6 Tensor product

1.2 Quantum Principles