QCOMP101: Mathematical requirements for quantum computing

Lotus Noir Quantum Computing Research Group

Based on:
Yanofsky, N. & Mannucci, M. (2008). *Quantum Computing for Computer Scientists.* Cambridge University Press

---

Lecture Outline: Quantum mechanics is different from most other branches of science in that it uses complex numbers in a fundamental way. Complex numbers are therefore absolutely essential to a basic understanding of quantum computation. Indeed quantum theory is cast in the language of complex vector spaces, we shall also introduce basic concepts of linear algebra in $\mathbb{C}^n$ during this lecture.

Contents

1 Complex Numbers

The original motivation for the introduction of complex numbers was the theory of algebraic equations, the part of algebra that seeks solutions of polynomial equations. It became apparent that there are plenty of cases in which no solution among familiar numbers set can be found. Here is the simplest example:

$$x^2 + 1 = 0 \tag{1}$$

Indeed, any $x^2 \in \mathbb{R}$ would be positive or zero. Hence no solution exists.

1.1 Basic definitions

Before building any new number system, it would be useful to remind ourselves of the other sets of numbers we usually work with:

- Positive numbers, $\mathbb{P} = \{1, 2, 3, ...\}$
- Natural numbers, $\mathbb{N} = \{0, 1, 2, 3, ...\}$
- Integers, $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$
- Rational numbers, $\mathbb{Q} = \{\frac{n}{m} | m \in \mathbb{Z}, n \in \mathbb{P}\}$
- Real numbers, $\mathbb{R} = \mathbb{R} \bigcup \{..., \sqrt{2}, ..., e, ..., \pi, ..., \frac{e}{\pi}, ...\}$

With $\mathbb{P} \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. In none of those familiar number systems can a valid solution to equation (1) be found. To be able to find a solution we need a number i such that $i^2 = -1$ or $i = \sqrt{-1}$.

Of course no such number exists in $\mathbb{R}$. Thus we will simply allow i to exists as an **imaginary number**, aside from its weird behavior when squared, i will behave just like an ordinary number.

We can add a real number to an imaginary number, for instance, $3 + 5 \times i$, and you get a hybrid entity which is not real nor imaginary and is called a **complex number**.

Definition 1.1. *A complex number is an expression such as:*

$$c = a + bi \tag{2}$$

*where $a, b \in \mathbb{R}$; a is called the **real part** of c, whereas b is its **imaginary part**. The set of all complex numbers will be denoted as $\mathbb{C}$ with $\mathbb{R} \subset \mathbb{C}$ (since real numbers are just complex number with an imaginary part equal to zero).*

1.2 Algebra of complex numbers

Since a complex number can be defined by two real numbers, let us define $c \in \mathbb{C}$ as an ordered pair of real:

$$c \longrightarrow (a, b) \tag{3}$$

Ordinary real numbers can then be identified with pairs $(a, 0)$ and imaginary numbers with pairs $0, b$, in particular $i \longrightarrow (0, 1)$.

Complex number **addition** performs componentwise:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \tag{4}$$

Whereas **multiplication** is a little trickier:

$$(a_1, b_1) \times (a_2, b_2) = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1) \tag{5}$$

Using addition and multiplication we thus can write any complex number number in the usual form such as:

$$c = (a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \times (0, 1) = a + bi \tag{6}$$

Exercise 1.1. Let $c_1 = (3, -2)$ and $c_2 = (1, 2)$. Calculate their product.

We have currently a set of numbers and two operations: addition and multiplication. Both operations are **commutative**, meaning that $\forall c_1, c_2 \in \mathbb{C}$ we have:

$$c_1 + c_2 = c_2 + c_1 \tag{7}$$

and

$$c_1 \times c_2 = c_2 \times c_1 \tag{8}$$

Both operation are also **associative**:

$$(c_1 + c_2) + c_3 = c_1 + (c_2 + c_3) \tag{9}$$

and

$$(c_1 \times c_2) \times c_3 = c_1 \times (c_2 \times c_3) \tag{10}$$

We can then show that multiplication **distributes** over addition, indeed $\forall c_1, c_2, c_3 \in \mathbb{C}$ we then have:

$$c_1 \times (c_2 + c_3) = (c_1 \times c_2) + (c_1 \times c_3) \tag{11}$$

Complex **subtraction** is straightforward:

$$c_1 c_2 = (a_1, b_1) - (a_2, b_2) = (a_1 - a_2, b_1 - b_2) \tag{12}$$

And finally we can express the **division** such as:

$$\frac{c_1}{c_2} = \frac{a_1 + b_1 i}{a_2 + b_2 i} = \frac{a_1 a_2 + b_1 b_2}{a_2^2 + b_2^2} + \frac{a_2 b_1 - a_1 b_2}{a_2^2 + b_2^2} \times i \tag{13}$$

Exercise 1.2. Let $c_1 = -2 + i$ and $c_2 = 1 + i$. Calculate $\frac{c_1}{c_2}$.

Real numbers have a unary operator (operator that need only one operand), the absolute value, given by:

$$|a| = +\sqrt{a^2} \tag{14}$$

We can define a generalization of this operation (14) to the complex domain by letting:

$$|c| = +\sqrt{a^2 + b^2} \tag{15}$$

This quantity is known as the **modulus** of a complex number. We can then rewrite the division(13) such as:

$$\frac{c_1}{c_2} = \frac{a_1 + b_1 i}{a_2 + b_2 i} = \frac{a_1 a_2 + b_1 b_2}{|c_2|^2} + \frac{a_2 b_1 - a_1 b_2}{|c_2|^2} \times i \tag{16}$$

Note that $|c_1 + c_2| \leq |c_1| + |c_2|$ and $|c_1|\,|c_2| = |c_1 c_2|$ which make sense geometrically.

There is a unary operation that plays a crucial role in the complex domain, we are already familiar with *"changing signs"* of real numbers, however there are two real numbers attached to a complex number. Therefore there are three ways of changing signs:

- **Changing signs of the real and imaginary parts** is done by multiplying by the number $-1 = (-1, 0)$.
- **Changing the sign of the imaginary part only** is known as **conjugation**. If $c = a+bi$ then the **conjugate** of c is $\overline{c} = a - bi$. Two numbers related by conjugation are said to be **complex conjugates** of each others.
- **Changing the sign of real part only** is defined by the operation $c \longrightarrow -\overline{c}$ (with $-\overline{c} = -a + bi$) has no particular name in the algebraic context but will be shown to be an **imaginary-axis reflection** in the Section 1.3.

Note that $\overline{c_1} + \overline{c_2} = \overline{c_1 + c_2}$ and $\overline{c_1} \times \overline{c_2} = \overline{c_1 \times c_2}$ and most importantly that for $c = a + bi$ we have $c \times \overline{c} = |c|^2 = a^2 + b^2$.

1.3 Geometry of complex numbers

It turns out that the significance of complex numbers extends far beyond the algebraic domain and make them equally useful in geometry and hence in physics. At the beginning of Section 1.2, we learned that a complex number is a pair of real numbers. This suggests a natural means of representation: real numbers are placed on the axis of a 2-dimensional plane, so pairs of real numbers correspond to points on the plane, or, equivalently, corresponds to **vectors** starting from the origin and pointing to that point.

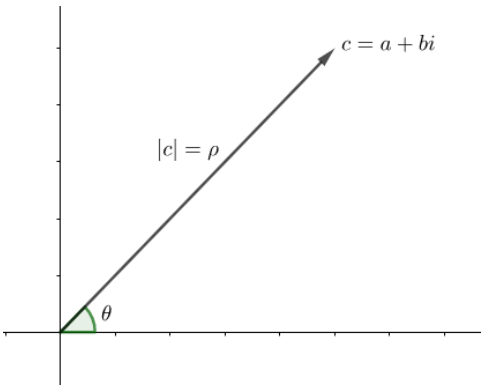

Figure 1: Complex plane

Thus the number $c = a + bi$ can be represented as a vector of coordinates (a, b) with the x axis being the **real axis** whereas the y-axis correspond to the **imaginary axis**. The vector length corresponds to the **modulus** $|c|$ which we will refer from now on as the **magnitude** ρ (to adjust to physics vocabulary) and the angle θ corresponds to the **phase** of c.

We can then express c in polar coordinates with its magnitude ρ and its phase θ such as:

$$(a, b) \longrightarrow (\rho, \theta) \tag{17}$$

With $\rho = \sqrt{a^2 + b^2}$ and $\theta = tan^{-1}(\frac{b}{a})$ which can be found via simple trigonometry. Note that we can go back to cartesian coordinates with $a = \rho \cos\theta$ and $b = \rho \sin\theta$. From a polar coordinates point of view, we consider that c_1 and c_2 have the same phases θ_1 and θ_2 if with $k \in \mathbb{Z}$ we have:

$$\theta_1 = \theta_2 \Leftrightarrow \theta_2 = \theta_1 + 2\pi k = \theta_1[2\pi] \tag{18}$$

Example 1.1. Are the numbers $(3, -\pi)$ and $(3, \pi)$ the same ? Indeed they are: their magnitude is the same and their phases differ by $(-\pi) - \pi = -2\pi = (-1)2\pi$, thus the phase $\theta_2 = \pi$ is equal to the the phase θ_1 modulo 2π such as $\theta_2 = \theta_1 + 2\pi k$ with $k = -1 \in \mathbb{Z}$.

The **multiplication** in polar coordinates of two complex numbers can be obtained simply by multiplying their magnitudes and adding their phases such as:

$$(\rho_1, \theta_1) \times (\rho_2, \theta_2) \longrightarrow (\rho_1\rho_2, \theta_1 + \theta_2) \tag{19}$$

In particular the multiplication of a complex number c by i has interesting properties since the magnitude of i is 1 and its phase is equal to $\frac{\pi}{4}[2\pi]$ radians or 90°. It will indeed result in a counterclockwise rotation of 90°.

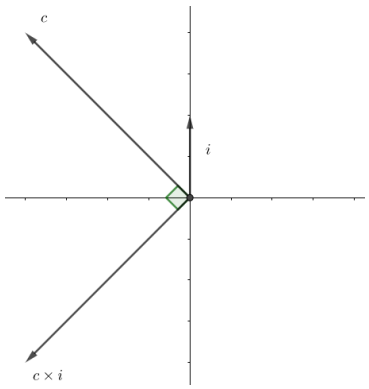

Figure 2: Multiplying by i results in a 90° rotation without change of magnitude.

We do not need any more fundamental knowledge about complex numbers to continue, just note that any complex number c can also be expressed in polar coordinates with its **exponential expression** $c = \rho e^{\theta}$.

2 Complex Vector Spaces

2.1 Definitions and properties

Notion goal 2.1. Quantum systems are described by using complex vector spaces and their evolution is represented by complex vector space's operations. Understanding definitions and properties is important to be able to grasp the nature of quantum states and operations in quantum computing.

Definition 2.1. *A **complex vector space** is a nonempty set of $\mathbb{V}$, whose elements we shall call vectors, with three operations:*

- *Addition:* $+ : \mathbb{V} \times \mathbb{V} \longrightarrow \mathbb{V}$
- *Negation:* $- : \mathbb{V} \longrightarrow \mathbb{V}$
- *Scalar multiplication:* $\cdot : \mathbb{C} \times \mathbb{V} \longrightarrow \mathbb{V}$

*and a distinguished element called the **zero vector** $0 \in \mathbb{V}$ in the set. These operations and zero must satisfy the following properties: $\forall V, W, X \in \mathbb{V}$ and $\forall c_1, c_2, c_2 \in \mathbb{C}$,*

1. *Commutativity of addition:* $V + W = W + V$
2. *Associativity of addition:* $(V + W) + X = V + (W + X)$
3. *Zero is an additive identity:* $V + 0 = V = 0 + V$

4. *Every vector has an inverse:* $V + (-V) = 0 = (-V) + V$
5. *Scalar multiplication has a unit:* $1 \cdot V = V$
6. *Scalar multiplication respects complex multiplication:* $c_1 \cdot (c_2 \cdot V) = (c_1 \times c_2) \cdot V$
7. *Scalar multiplication distributes over addition:* $c \cdot (V + W) = c \cdot V + c \cdot W$
8. *Scalar multiplication distributes over complex addition:* $(c_1 + c_2) \cdot V = c_1 \cdot V + c_2 \cdot V$

Any set that has an addition operation, an inverse operation and a zero element that satisfies properties 1, 2, 3 and 4 is called an **Abelian group**. If there is a scalar multiplication that satisfies all the properties, then the set with the operations is called a **complex vector space**. Even if our main concern is complex vector spaces, we can gain much intuition from real vector spaces.

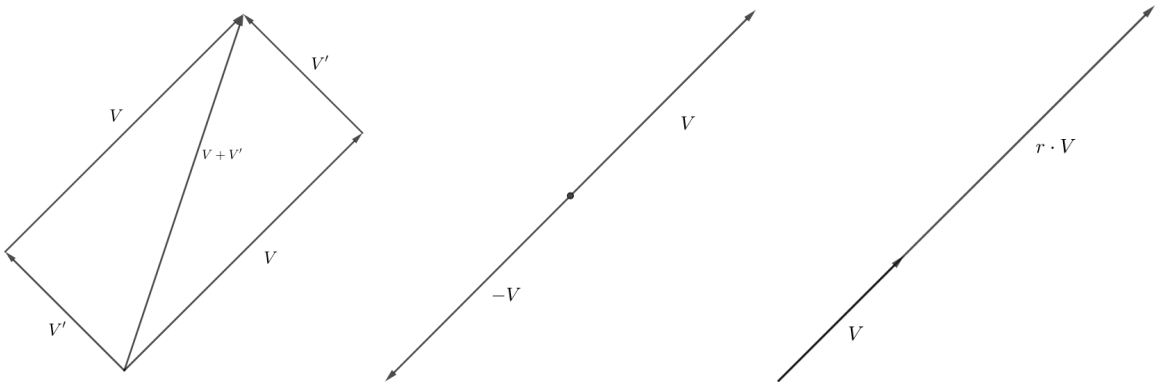

Figure 3: We can show using $\mathbb{R}^2$ as example that vector addition follows the parallelogram rule (left); the geometric interpretation of inverse vector (middle); and a real multiple of a vector (right).

Example 2.1. $\mathbb{C}^{m\times n}$, the set of all m-by-n matrices with complex entries, is a complex vector space.

For a given $A \in \mathbb{C}^{m\times n}$, we denote the complex entry in the jth row and the kth column as $A[j,k]$or $c_{j,k}$. We shall denote the jth row as $A[j,-]$ and the kth column as $A[-,k]$.

We will define three operations on $\mathbb{C}^{m\times n}$:

- The **transpose** of A, denoted A^T, is defined as $A^T[j,k] = A[k,j]$
- The **conjugate** of A, denoted $\overline{A}$, is defined as $\overline{A}[j,k] = \overline{A[j,k]}$
- The **adjoint** of A, denoted $A^\dagger$, is defined as $A^\dagger = (\overline{A}^T) = \overline{(A^T)}$ or $A^\dagger[j,k] = \overline{A[k,j]}$.

These operations satisfy the following properties $\forall c \in \mathbb{C}$ and $\forall A, B \in \mathbb{C}^{m\times n}$:

1. Transpose is idempotent: $(A^T)^T = A$
2. Transpose respects addition: $(A + B)^T = A^T + B^T$
3. Transpose respects scalar multiplication: $(c \cdot A)^T = c \cdot A^T$
4. Conjugate is idempotent: $\overline{\overline{A}} = A$
5. Conjugate respects addition: $\overline{A + B} = \overline{A} + \overline{B}$

6. Conjugate respects scalar multiplication: $\overline{c \cdot A} = \overline{c} \cdot A$
7. Adjoint is idempotent: $(A^\dagger)^\dagger = A$
8. Adjoint respects addition: $(A + B)^\dagger = A^\dagger + B^\dagger$
9. Adjoint respects scalar multiplication $(c \cdot A)^\dagger = \overline{c} \cdot A^\dagger$

The **matrix multiplication** is the binary operation $* : \mathbb{C}^{m\times n} \times \mathbb{C}^{n\times p} \longrightarrow \mathbb{C}^{m\times p}$ defined such as:

$$(A * B)[j,k] = \sum_{h=0}^{n-1} (A[j,h] \times B[h,k]) \tag{20}$$

As we will mainly work with **square matrices**, we will shows that matrix multiplication satisfies the following properties: $\forall\ A, B, C \in \mathbb{C}^{n\times n}$,

1. Matrix multiplication is associative: $(A * B) * C = A * (B * C)$
2. Matrix multiplication has I_n as a unit: $I_n * A = A = A * I_n$
3. Matrix multiplication distributes over addition: $A * (B + C) = (A * B) + (A * C)$ and $(B + C) * A = (B * A) + (C * A)$
4. Matrix multiplication respects scalar multiplication: $c \cdot (A * B) = (c \cdot A) * B = A * (c \cdot B)$
5. Matrix multiplication relates to the transpose: $(A * B)^T = B^T * A^T$
6. Matrix multiplication respects the conjugate: $\overline{A * B} = \overline{A} * \overline{B}$
7. Matrix multiplication relates to the adjoint: $(A * B)^\dagger = B^\dagger * A^\dagger$

Note that **commutativity is not a property** of matrix multiplication. This fact will be very important in quantum mechanics.

Let $A \in \mathbb{C}^{m\times n}$ and $B \in \mathbb{C}^n$, $A * B \in \mathbb{C}^n$,

A represents the function $A : \mathbb{C}^n \longrightarrow \mathbb{C}^n$.

As the elements of $\mathbb{C}^n$ will be our way to describe the states of a quantum system, some suitable elements of $\mathbb{C}^{m\times n}$ will correspond to the changes that occur to the states of a quantum system. Given a state $X \in \mathbb{C}^n$ and a matrix $A \in \mathbb{C}^{m\times n}$, we shall form another state of the system $A * X \in \mathbb{C}^n$. We say that the algebra of matrices "**acts**" on the vectors to yield new vectors.

Definition 2.2. *Given two complex vector spaces $\mathbb{V}$ and $\mathbb{V}'$, we say that $\mathbb{V}$ is a **complex subspace** of $\mathbb{V}'$ if $\mathbb{V}$ is a subset of $\mathbb{V}'$ and:*

1. *$\mathbb{V}$ is closed under addition: $\forall\ V_1, V_2 \in \mathbb{V}$, $V_1 + V_2 \in \mathbb{V}$*
2. *$\mathbb{V}$ is closed under scalar multiplications: $\forall\ c \in \mathbb{C}$ and $\forall V \in \mathbb{V}$, $c \cdot V \in \mathbb{V}$*

Definition 2.3. *Let $\mathbb{V}$ and $\mathbb{V}'$ be two complex vector spaces. A **linear map** from $\mathbb{V}$ to $\mathbb{V}'$ is a function $f : \mathbb{V} \longrightarrow \mathbb{V}'$ such that $\forall V, V_1, V_2 \in \mathbb{V}$ and $\forall c \in \mathbb{C}$,*

1. *f respects the addition: $f(V_1 + V_2) = f(V_1) + f(V_2)$*
2. *f respects the scalar multiplication: $f(c \cdot V) = c \cdot f(V)$*

A linear map $F : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ such that for $A \in \mathbb{C}^{m\times n}$ and $V \in \mathbb{V}$, $F(V) = A * V$ will be called an **operator** and be represented by matrix A. Note that several matrices might represent the same operator.

Definition 2.4. *$\mathbb{V}$ and $\mathbb{V}'$ are **isomorphic** if there is a one-to-one **linear map** $F : \mathbb{V} \longrightarrow \mathbb{V}'$. Such a map is called an **isomorphism**.*

It means that the name of the elements of the vector spaces are renamed but the structure of the vector spaces are the same, these are said "**essentially the same**" or "**the same up to isomorphism**".

Example 2.2. *$Poly_n$*, the set of complex polynomials of degree n, then $n+1$ coefficient and $\mathbb{C}^{n+1}$ are isomorphic since representing a polynomial is done through storing its complex coefficients in a $n+1$ array.

What we have learned 2.1. Through this part, we described the basic operations in $\mathbb{C}^n$ and their properties as well as some basic definition about complex vector space, in particular:

- A function $f : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ applied to a vector $V \in C^n$ can be represented as a matrix A which we will call **operator** such as $f(V) = A * V$. In the next lectures, we will represents quantum systems as vectors of complex numbers and we will describe the operations on them by those operator matrices.
- We have learned that we can compare the vector spaces and we defined that vector spaces are **isomorphic** when they share the same structure. We also discovered **vector subspaces** which are subsets of vector spaces, adding or applying scalar multiplication on vectors in this subspace **must** yield vectors that are also part of the same subspace.

2.2 Basis and dimension

A basis of a vector space is a set of vectors of that vector space that is special in the sense that all other vectors can be uniquely written in terms of these basis vectors.

Notion goal 2.2. As we saw before, quantum systems are represented by complex vectors, the notion of basis will offer a very convenient way to represent quantum systems in superposition as a linear combination of possible outcome states defined by elements of the basis of a complex vector space.

Definition 2.5. *Let $\mathbb{V}$ be a complex vector space, $V \in \mathbb{V}$ is a **linear combination** of the vectors $V_0, V_(1), ..., V_{n-1} \in \mathbb{V}$ if V can be written as:*

$$V = c_0 \cdot V_0 + c_1 \cdot V_1 + ... + c_{n-1} \cdot V_{n-1} \tag{21}$$

for some $c_0, c_1, ..., c_{n-1} \in \mathbb{C}$.

A set $\{V_0, V_1, ..., V_{n-1}\} \in \mathbb{V}$ is called **linearly independent** if:

$$0 = c_0 \cdot V_0 + c_1 \cdot V_1 + ... + c_{n-1} \cdot V_{n-1} \Rightarrow c_0 = c_1 = ... = c_{n-1} = 0 \tag{22}$$

That means that the only way that linear combination can be equal to the 0 vector is that all the c_j are zero. This also means that the vectors in $\{V_0, V_1, ..., V_{n-1}\}$ cannot be written as a combination of the others in the set.

Example 2.3.

$$\left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\} \tag{23}$$

is **linearly independent** because the only way that

$$0 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = x \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + z \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \tag{24}$$

is that $x = y = z = 0$

Example 2.4.

$$\left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 2 \\ -1 \\ -1 \end{pmatrix} \right\} \tag{25}$$

is **linearly dependent** because

$$0 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = x \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + z \begin{pmatrix} 2 \\ -1 \\ -1 \end{pmatrix} \tag{26}$$

can be solved with $\begin{cases} x = 3 \\ y = -3 \\ z = -1 \end{cases}$

Definition 2.6. *A set $B = \{V_0, V_1, ..., V_{n-1}\} \subseteq \mathbb{V}$ is called a **basis** of the (complex) vector space $\mathbb{V}$ if both:*

1. *every $V \in \mathbb{V}$ can be written as a linear combination of vectors from B*
2. *B is linearly independent*

Even if many sets can form a basis, it is easier to work with **canonical basis** (also called standard basis).

Example 2.5. The canonical basis of $\mathbb{C}^n$ is:

$$\left\{ E_0 = \begin{pmatrix} 1 \\ 0 \\ ... \\ 0 \end{pmatrix} \quad E_1 = \begin{pmatrix} 0 \\ 1 \\ ... \\ 0 \end{pmatrix} \quad ... \quad E_{n-1} = \begin{pmatrix} 0 \\ 0 \\ ... \\ 1 \end{pmatrix} \right\} \tag{27}$$

Every vector $V \in \mathbb{C}^n$ can be written as $V = \sum_{i=0}^{n-1} c_i E_i$ for $c \in \mathbb{C}^n$.

Proposition 2.1. For every vector space, every basis has the same number of vectors.

Definition 2.7. *The **dimension** of a vector space is the number of elements in a basis of the vector space.*

Example 2.6. Let us cite some dimension examples:

- $dim(\mathbb{R}^3) = 3$ as a real vector space.
- $dim(\mathbb{C}^n) = n$ as a complex vector space, it is however of dimension $2n$ as a real vector space since every complex is described by two real numbers.
- $dim(\mathbb{C}^{m \times n}) = m \times n$ as a complex vector space.
- $dim(\mathbb{V} \times \mathbb{V}') = dim(\mathbb{V}) + dim(\mathbb{V}')$.

Proposition 2.2. Any two vector spaces that have the **same dimensions** are **isomorphic**. In particular for each n, there is essentially only one complex vector space that is of dimension n: $\mathbb{C}^n$.

Sometime we shall use more than one basis for a single vector space, consider the basis

$$B = \left\{ \begin{pmatrix} 1 \\ -3 \end{pmatrix} \quad \begin{pmatrix} -2 \\ 4 \end{pmatrix} \right\} \subseteq \mathbb{R}^2 \tag{28}$$

The vector $V = \begin{pmatrix} 7 \\ -17 \end{pmatrix}$ can be written as $V = 3\begin{pmatrix} 1 \\ -3 \end{pmatrix} - 2\begin{pmatrix} -2 \\ 4 \end{pmatrix}$ thus we say $V_B = \begin{pmatrix} 3 \\ -2 \end{pmatrix}$.

If C is the canonical basis of $\mathbb{R}^2$ then

$$V = \begin{pmatrix} 7 \\ -17 \end{pmatrix} = 7\begin{pmatrix} 1 \\ 0 \end{pmatrix} - 17\begin{pmatrix} 0 \\ 1 \end{pmatrix} \Rightarrow V_C = V = \begin{pmatrix} 7 \\ -17 \end{pmatrix} \tag{29}$$

Let us consider another basis of $\mathbb{R}^2$: $D = \left\{ \begin{pmatrix} -7 \\ 9 \end{pmatrix} \quad \begin{pmatrix} -5 \\ 7 \end{pmatrix} \right\}$.

A **transition matrix** from basis B to basis D is noted $M_{D \leftarrow B}$ such as:

$$V_D = M_{D \leftarrow B} * V_B = \begin{pmatrix} 2 & -\frac{3}{2} \\ -3 & \frac{5}{2} \end{pmatrix} * \begin{pmatrix} 3 \\ -2 \end{pmatrix} = \begin{pmatrix} 9 \\ -14 \end{pmatrix} \tag{30}$$

There are standard algorithms to find transition matrices, however we do not need to know how to do use them for this lecture.
In $\mathbb{R}^2$, the transition matrix from the canonic basis $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ to the other basis $\left\{ \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \right\}$ is the **Hadamard matrix** H:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \tag{31}$$

The Hadamard matrix plays a major role in quantum computing. Note that $H * H = I_2$ meaning that the transition is reversible.

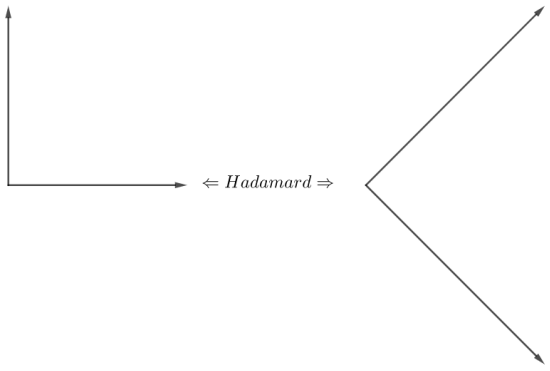

Figure 4: The Hadamard matrix as a transition between two bases.

What we have learned 2.2. In this section we have introduced the notion of basis, which are key to understand the notion of dimension of vector spaces in particular:

- Every vector of a vector space can be expressed as a **linear combination** of elements belonging to the basis of this vector space. Canonical basis are much easier to work with in most cases.
- Sometimes it is more convenient to switch to another base to simplify calculations during a specific operation, to perform this change of basis, we use **transition matrices**.

2.3 Inner products and Hilbert spaces

Notion goal 2.3. The notion of inner product is extremely useful to manipulate elements of vector spaces, hence it is also useful to perform operations on quantum systems. It introduces the notion of Hilbert space, which is frequently used in most of the quantum computing literature, from now on, we will only work on Hilbert spaces.

Definition 2.8. *An **inner product** (or dot product) on a complex vector space $\mathbb{V}$ is a function $\langle -, - \rangle : \mathbb{V} \times \mathbb{V} \longrightarrow \mathbb{C}$ which satisfies the following conditions $\forall\ V, V_1, V_2, V_3, V_4 \in \mathbb{V}$ and $\forall c \in \mathbb{C}$:*

1. *Non degenerate: $\langle V, V \rangle \geq 0$ if $V \neq 0$*
2. *Respects addition: $\langle V_1 + V_2, V_3 \rangle = \langle V_1, V_3 \rangle + \langle V_2, V_3 \rangle$ and $\langle V_1, V_2 + V_3 \rangle = \langle V_1, V_2 \rangle + \langle V_1, V_3 \rangle$*
3. *Respects scalar multiplication: $\langle c \cdot V_1, V_2 \rangle = \overline{c} \times \langle V_1, V_2 \rangle$ and $\langle V_1, c \cdot V_2 \rangle = c \times \langle V_1, V_2 \rangle$*
4. *Skew symmetric: $\langle V_1, V_2 \rangle = \overline{\langle V_2, V_1 \rangle}$*

Note that with property 4 we can show that the inner product of a complex vector with itself is a real number: $\langle V, V \rangle = \overline{\langle V, V \rangle}$ and $x = \overline{x} \Leftrightarrow x \in \mathbb{R}$.

Definition 2.9. *A **inner product space** is a vector space along with an inner product.*

Example 2.7. Let us list some example of inner product spaces:

- $\mathbb{R}^n$: the inner product is defined as $\langle V_1, V_2 \rangle = V_1^T * V_2$
- $\mathbb{C}^n$: the inner product is defined as $\langle V_1, V_2 \rangle = V_1^\dagger * V_2$ with $V^\dagger = (\overline{V})^T$
- $\mathbb{R}^{n \times n}$: the inner product is defined as $\langle A, B \rangle = Trace(A^T * B)$
- $\mathbb{C}^{n \times n}$: the inner product is defined as $\langle A, B \rangle = Trace(A^\dagger * B)$

Definition 2.10. *For every complex inner product space $\mathbb{V}, \langle -, - \rangle$, we can define a **norm** (or length) which is a function $|\ | : \mathbb{V} \longrightarrow \mathbb{R}$ defined as:*

$$|V| = \sqrt{\langle V, V \rangle} \tag{32}$$

and satisfies the following properties $\forall\ V, W \in \mathbb{V}$ and $c \in \mathbb{C}$:

1. *Non degenerate: $|V| \geq 0$ if $V \neq 0$*
2. *Triangle inequality: $|V + W| \leq |V| + |W|$*
3. *Respects scalar multiplication: $|c \cdot V| = |c| \times |V|$*

Definition 2.11. *For every complex inner product space $\mathbb{V}, \langle -, - \rangle$, we can define the **distance function** $d(\ ,\ ) : \mathbb{V} \times \mathbb{V} \longrightarrow \mathbb{R}$ defined as:*

$$d(V_1, V_2) = |V_1 - V_2| = \sqrt{\langle V_1 - V_2, V_1, V_2 \rangle} \tag{33}$$

and satisfies the following properties $\forall U, V, W \in \mathbb{V}$ and $c \in \mathbb{C}$:

1. *Non degenerate: $d(V, W) \geq 0$ if $V \neq W$*
2. *Triangle inequality: $d(U, V) \leq d(U, W) + d(W, V)$*
3. *Symmetric: $d(V, W) = d(W, V)$*

Definition 2.12. *Two vectors V_1 and V_2 in an inner product space $\mathbb{V}, \langle -, - \rangle$ are **orthogonal** if $\langle V_1, V_2 \rangle = 0$.*

Definition 2.13. *A basis $B = \{V_0, V_1, ..., V_{n-1}\}$ for an inner product space $\mathbb{V}, \langle -, - \rangle$ is called an* ***orthogonal basis*** *if the vector are pairwise orthogonal to each other, i.e, $j \neq k \Leftrightarrow \langle j, k \rangle = 0$. An orthogonal basis is called an* ***orthonormal basis*** *if every vector in the basis is of norm 1,*

$$\langle V_j, V_k \rangle = \delta_{j,k} = \begin{cases} 1 \text{ if } j = k \\ 0 \text{ if } j \neq k \end{cases} \tag{34}$$

$\delta_{j,k}$ is called the ***Kronecker delta function****.*

In $\mathbb{R}^2$, $\langle V, V' \rangle = |V|\,|V'| \cos\theta$ and when $|V'| = 1$ we have $\langle V, V' \rangle = |V| \cos\theta$ which corresponds to the length of the projection of V onto V'.

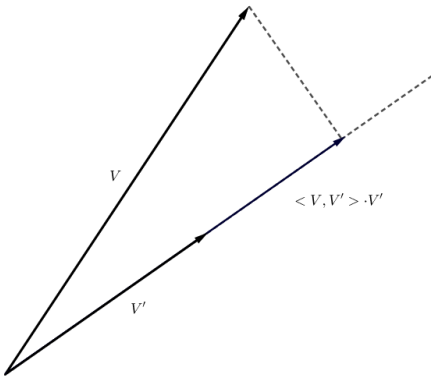

Figure 5: The projection of V onto V'.

Hence, $\langle V, V' \rangle \cdot V'$ is the vector V' extended (or reduced) to meet the projecton of V onto V'. What does it means in terms of $\mathbb{R}^3$? Let $V = (r_9, r_1, r_2)^T \in \mathbb{R}^3$ and $\{E_0, E_1, E_2\} \in \mathbb{R}^3$. Then:

$$V = \begin{pmatrix} r_0 \\ r_1 \\ r_2 \end{pmatrix} = \langle E_0, V \rangle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \langle E_1, V \rangle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \langle E_2, V \rangle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \tag{35}$$

In general, for any $V \in \mathbb{R}^n$, $V = \sum_{j=0}^{n-1} \langle E_i, V \rangle E_i$. We shall use the intuition given by $\mathbb{R}^3$ and $\mathbb{R}^n$ to understand this type of **decomposition of vectors in sums of canonical vectors** for other vector spaces.

Proposition 2.3. In $\mathbb{C}^n$, any V can be written as:

$$V = \langle E_0, V \rangle E_0 + \langle E_1, V \rangle E_1 + ... + \langle E_{n-1}, V \rangle E_{n-1} \tag{36}$$

Note that this is true for any orthonormal basis, not just the canonical one.

Definition 2.14. *Within an inner product space $\mathbb{V}, \langle\ ,\ \rangle$ (with the derived norm and a distance function), a sequence of vectors $V_0, V_1, V_2, ...$ is called a* ***Cauchy sequence*** *if $\forall \epsilon \geq 0, \exists N_0 \in \mathbb{N}$ such that:*

$$\forall m, n \geq N_0,\ d(V_m, V_n) < \epsilon \tag{37}$$

Definition 2.15. *A complex inner product space $\mathbb{V}, \langle\ ,\ \rangle$ is called* ***complete*** *if for any Cauchy sequence of vectors $V_0, V_1, ...$ there exists a vector $V \in \mathbb{V}$ such that:*

$$\lim_{n \to \infty} |V_n - V| = 0 \tag{38}$$

The intuition behind this is that a vector space with an inner product is complete if any sequence accumulating somewhere converges to a specific point.

Definition 2.16. *A **Hilbert space** is a complex inner product space that is complete.*

If completeness seems like an overly complicated notion, given the scope of our lecture, we do not need it thanks to the following proposition.

Proposition 2.4. Every inner product on a finite-dimensional complex vector space is automatically complete, hence every finite-dimensional complex vector space with an inner product is automatically a Hilbert space.

Quantum computing in this lecture will only deal with finite-dimensional vector spaces and we do not have to concern ourselves with the notion of completeness.

What we have learned 2.3. Through this part we understood the notion of norm, distance and projections using the inner product of a (complex) vector space, along with the notion of completeness, those allowed us to precisely define **Hilbert spaces**. We will see again the inner product for the notion of transition amplitude, which represents the collapse of a quantum system to a possible outcome state as a inner product.

2.4 Eigenvalues and eigenvectors

Notion goal 2.4. The notion of eigenvalues and eigenvectors will be useful to us in association of hermitian matrices (next section), in particular every physical observable of a quantum system have a corresponding hermitian matrix and measurement of that observable leads to a state that is represented by one eigenvector associated to this matrix.

Example 2.8. Consider the $\mathbb{R}^{2\times 2}$ matrix

$$\begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix} \tag{39}$$

Notice that:

$$\begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 3 \end{pmatrix} = 3 \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} \tag{40}$$

Multiplying our matrix by this vector is nothing more then multiplying the vector by a scalar. In other words, when this matrix acts on this vector, it does not change the direction of the vector but only its length.

Of course this is not always true for every vector, nor is it true for every matrix. However when it is true, we assign special names to such scalars and vectors.

Definition 2.17. *For a matrix $A \in \mathbb{C}^{n\times n}$, if there is a number $c \in \mathbb{C}$ and a vector $V \neq 0$ in $\mathbb{C}^n$ such that:*

$$AV = c \cdot V \tag{41}$$

*this c is called an **eigenvalue** of A and V is called an **eigenvector** of A associated with c. ("eigen-" is a German prefix that indicates possession.)*

If a matrix A has eigenvalue c_0 with eigenvector V_0, then $\forall\ c \in \mathbb{C}$ we have

$$A(cV_0) = cAV_0 = cc_0 = c_0(cV_0) \tag{42}$$

which shows that cV_0 is also an eigenvector of A with eigenvalue c_0. If cV_0 and $c'V_0$ are two such eigenvectors, then because

$$A(cV_0 + c'V_0) = AcV_0 + Ac'V_0 = cAV_0 + c'AV_0 = c(c_0V_0) + c'(c_0V_0) = (c + c')(c_0V_0) \tag{43}$$

we see that athe addition of two such eigenvectors is also an eigenvector. We can conclude the following proposition:

Proposition 2.5. Every eigenvector determines a complex subvector of the vector space. This space is known as the **eigenspace** associated to the given eigenvector.

Some matrices have many eigenvalues and eigenvector while other have none.

What we have learned 2.4. We saw the definition of eigenvalues and eigenvectors, and that since the sum and scalar multiplication of eigenvectors still yields other eigenvectors, they form by definition a vector subspace called **eigenspace**.

2.5 Hermitian and unitary matrices

Notion goal 2.5. As we saw previously, all operations on quantum systems will be represented by matrices, for example observables (that we will cover in next lectures) of quantum systems are represented by hermitian matrices, whereas any operation performed by quantum gates have to be represented by unitary matrices.

A matrix $A \in \mathbb{R}^n$ is called **symmetric** if $A^T = A$. In other words, $A[j,k] = A[k,j]$. And we can generalize this notion complex numbers such as:

Definition 2.18. *A matrix $A \in \mathbb{C}^{n\times n}$ is called **hermitian** if $A^\dagger = A$. In other words, $A[j,k] = \overline{A[k,j]}$ with $A^\dagger = (\overline{A})^T$.*

Notice from this definition that the **elements** along the (main) **diagonal** of an hermitian matrix must be **real**.

Definition 2.19. *If A is a hermitian matrix then the operator it represents is called **self-adjoint**.*

Proposition 2.6. If a is a hermitian n-by-n matrix, then $\forall V, V' \in \mathbb{C}^n$ we have:

$$\langle AV, V' \rangle = \langle V, AV' \rangle \tag{44}$$

Which can be proved easily: $\langle AV, V' \rangle = (AV)^\dagger * V' = V^\dagger A^\dagger V' = V^\dagger * AV' = \langle V, AV' \rangle$

Proposition 2.7. If A is **hermitian**, then all its **eigenvalues** are **real**. Indeed it can be easily shown that with an eigenvalue $c \in \mathbb{C}$ and $V \in \mathbb{C}^n$ an eigenvector we have

$$c \langle V, V \rangle = \langle V, AV \rangle = \langle AV, V \rangle = \langle cV, V \rangle = \overline{c} \langle V, V \rangle \tag{45}$$

And because V is nonzero, $c = \overline{c} \Rightarrow c \in \mathbb{R}$.

Proposition 2.8. For a given hermitian matrix, distinct eigenvectors that have distinct eigenvalues are orthogonal.

Definition 2.20. *A **diagonal matrix** is a square matrix whose only nonzero entries are on the (main) diagonal. All entries of the diagonal are zero.*

Proposition 2.9. (The Spectral Theorem for Finite-Dimensional Self-Adjoint Operators) Every self-adjoint operator A on a **finite-dimensional** complex vector space $\mathbb{V}$ can be represented by a **diagonal matrix** whose diagonal entries are the **eigenvalues** of A and whose eigenvectors form an orthonormal basis for $\mathbb{V}$ which is called an **eigenbasis**.

Definition 2.21. *A matrix A is **invertible** if there exists a matrix A^{-1} such that:*

$$A * A^{-1} = A^{-1} * A = I_n \tag{46}$$

Unitary matrices are a type of invertible matrix. They are invertible and their **inverse is their adjoint**. This fact ensure that unitary matrices "preserve the geometry" of the space on which it is acting.

Definition 2.22. *A matrix $U \in \mathbb{C}^{n\times n}$ is **unitary** if:*

$$U * U^\dagger = U^\dagger * U = I^n \tag{47}$$

Show that the matrix P is unitary for any θ.

$$P = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Proposition 2.10. Unitary matrices **preserves inner product**, i.e, if U is unitary then $\forall\ V, V' \in \mathbb{C}^n$ we have $\langle UV, UV' \rangle = \langle V, V' \rangle$.

Because unitary matrices preserves inner product, they also preserves norms.

$$|UV| = \sqrt{\langle UV, UV \rangle} = \sqrt{\langle V, V \rangle} = |V| \tag{48}$$

In particular, if $|V| = 1$, then $|UV| = 1$. Consider the set of all vectors that have a norm of 1, they form a ball around the origin (the zero of the vector space), we call this ball the **unit sphere**.

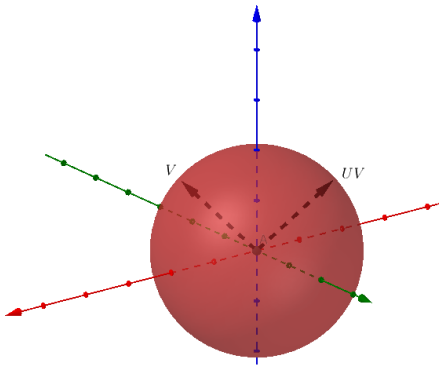

Figure 6: The unit sphere and the action of U on V.

If V is a vector on the unit sphere, UV is also on the unit sphere. A **unitary matrix is a way of rotating the unit sphere**.

If U is unitary and $UV = V'$, then we can easily multiply both sides of the equation by $U^\dagger$ to get $U^\dagger UV = U^\dagger V' = V$, then $U^\dagger$ can "undo" the action of the operator U on V, we say that this action is "**reversible**".

What we have learned 2.5. Through this section we defined hermitian matrices, which, when representing an operator, are called **self-adjoint** operators as well as unitary matrices that can be used to rotate the unit sphere. In particular:

- A quantum bit, that for now we will define simply as the smallest possible quantity of information supported by a quantum system, can be implemented with a **polarized photon** which can be represented by a unit sphere and a polarization vector, applying a quantum gate on this quantum bit will be done by applying a rotation on this photon, this operation will be represented using a unitary matrix.
- The **reversible** property of actions performed by unitary matrices on vectors will be a very useful notion when we will introduce quantum gates.
- The variant of spectral theorem we introduced will be useful when we will define **observables** of quantum systems.

2.6 Tensor product of vector spaces

Notion goal 2.6. The notion of tensor product is critical to represent the concept of quantum entanglement which is a very important effect in quantum physics and computing.

In this section we study the tensor product which is an important method of combining vector spaces. If $\mathbb{V}$ describes a quantum system and $\mathbb{V}'$ describes another, then their tensor product describes both quantum systems as one. The tensor product is therefore the most fundamental building operation of quantum systems.

Given two vector spaces $\mathbb{V}$ and $\mathbb{V}'$, we shall form the **tensor product** of two vector spaces, and denote it $\mathbb{V} \otimes \mathbb{V}'$. The tensor product is generated by the set of tensors:

$$\{V \otimes V' \mid V \in \mathbb{V} \text{ and } V' \in \mathbb{V}'\} \tag{49}$$

where $\otimes$ is just a symbol. A typical element of $\mathbb{V} \otimes \mathbb{V}'$ looks like this:

$$\sum_{i=0}^{n-1} c_i(V_i \otimes V_i') = c_0(V_0 \otimes V_0') + c_1(V_1 \otimes V_1') + ... + c_{n-1}(V_{n-1} \otimes V_{n-1}') \tag{50}$$

The operations on this vector space are straightforward. For a given $\sum_{i=0}^{p-1} c_i(V_i \otimes V_i')$ and $\sum_{i=0}^{q-1} c_i(V_i \otimes V_i')$, the **addition** is defined as:

$$\sum_{i=0}^{p-1} c_i(V_i \otimes V_i') + \sum_{i=0}^{q-1} c_i(V_i \otimes V_i') \tag{51}$$

And the **scalar multiplication** for a given $c \in \mathbb{C}$ is:

$$c \cdot \sum_{i=0}^{p-1} c_i(V_i \otimes V_i') = \sum_{i=0}^{q-1} (c \times c_i)(V_i \otimes V_i') \tag{52}$$

We impose the following rewriting rules for this vector space:

1. The tensor must respect addition in both $\mathbb{V}$ and $\mathbb{V}'$:

$$(V_i + V_j) \otimes V_k' = V_i \otimes V_k' + V_j \otimes V_k' \tag{53}$$

$$V_i \otimes (V_j' \otimes V_k') = V_i \otimes V_j' + V_i \otimes V_k' \tag{54}$$

2. The tensor must respect the scalar multiplication in both $\mathbb{V}$ and $\mathbb{V}'$:

$$c \cdot (V_j \otimes V_k') = (c \cdot V_j) \otimes V_k' = V_j \otimes (c \cdot V_k') \tag{55}$$

By following these rewriting rules and setting elements equal to each other, we form $\mathbb{V} \otimes \mathbb{V}'$.

Let $B = \{B_0, B_1, ..., B_{m-1}\}$ the basis of $\mathbb{V}$ and $B' = \{B_0', B_1', B_{n-1}\}$ the basis of $\mathbb{V}'$, then the basis of $\mathbb{V} \otimes \mathbb{V}'$ is the set of vectors $\{B_j \otimes B_k' \mid j = 0, 1, ..., m-1 \text{ and } k = 0, 1, ..., n-1\}$. Thus $dim(\mathbb{V} \otimes \mathbb{V}') = dim(\mathbb{V}) \times dim(\mathbb{V}') = m \times n$, it is isomorphic to $\mathbb{C}^{m \times n}$ and every vector $\sum_{i=0}^{p-1} c_i(V_i \otimes V_i') \in \mathbb{V} \otimes \mathbb{V}'$ can be written as:

$$c_{0,0} + (B_0 \otimes B_0') + c_{1,0}(B_1 \otimes B_0') + ... + c_{m-1,n-1}(B_{m-1}, B_{n-1}') \tag{56}$$

$\mathbb{V} \otimes \mathbb{V}'$ is to be thought of as the vector space whose basic states are pairs of states, one from system $\mathbb{V}$ and one from system $\mathbb{V}'$.

Given a vector $c_0B_0 + c_1B_1 + .. + c_{m-1}B_{m-1} \in \mathbb{V}$ and a vector $c'_0B'_0 + c'_1B'_1 + ... + c_{n-1}B'_{n-1} \in \mathbb{V}'$, we can associate the following element to $\mathbb{V} \otimes \mathbb{V}'$:

$$(c_0 \times c'_0)(B_0 \otimes B'_0) + (c_1 \times c'_1)(B_0 \otimes B'_1) + ... + (c_{m-1} \times c'_{n-1})(B_{m-1} \otimes B_{n-1}) \tag{57}$$

The **tensor product of two vectors** is defined as follow:

$$\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} \otimes \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_0 \cdot \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} \\ a_1 \cdot \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} \\ a_2 \cdot \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} \\ a_3 \cdot \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} a_0b_0 \\ a_0b_1 \\ a_0b_2 \\ a_1b_0 \\ a_1b_1 \\ a_1b_2 \\ a_2b_0 \\ a_2b_1 \\ a_2b_2 \\ a_3b_0 \\ a_3b_1 \\ a_3b_2 \end{pmatrix} \tag{58}$$

Example 2.9. Consider $V = \begin{pmatrix} 8 \\ 12 \\ 6 \\ 12 \\ 18 \\ 9 \end{pmatrix} \in \mathbb{C}^6 = \mathbb{C}^2 \otimes \mathbb{C}^3$, V can be expressed as $\begin{pmatrix} 2 \\ 3 \end{pmatrix} \otimes \begin{pmatrix} 4 \\ 6 \\ 3 \end{pmatrix}$

Example 2.10. In contrast, $\begin{pmatrix} 8 \\ 0 \\ 0 \\ 0 \\ 0 \\ 18 \end{pmatrix} \in \mathbb{C}^6 = \mathbb{C}^2 \otimes \mathbb{C}^3$ cannot be written as $\begin{pmatrix} x \\ y \end{pmatrix} \otimes \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} xa \\ xb \\ xc \\ ya \\ yb \\ yc \end{pmatrix}$ since $yc \neq 0$ and $xa \neq 0$ but $ya = 0$ which is impossible. But it can be written as a sum of tensor products such as:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 8 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 6 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix} \tag{59}$$

We shall call a vector that can be written as the tensor of two vectors **separable**. And a vector that cannot be written as the tensor of two vector but can be written as the nontrivial sum of such tensors shall be called **entangled**.

We also need to know the **tensor product of two matrices** which is defined as:

$$A \otimes B = \begin{pmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{pmatrix} \otimes \begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} \\ b_{1,0} & b_{1,1} & b_{1,2} \\ b_{2,0} & b_{2,1} & b_{2,2} \end{pmatrix}$$

$$= \begin{pmatrix} a_{0,1} \cdot \begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} \\ b_{1,0} & b_{1,1} & b_{1,2} \\ b_{2,0} & b_{2,1} & b_{2,2} \end{pmatrix} & a_{0,1} \cdot \begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} \\ b_{1,0} & b_{1,1} & b_{1,2} \\ b_{2,0} & b_{2,1} & b_{2,2} \end{pmatrix} \\ a_{1,0} \cdot \begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} \\ b_{1,0} & b_{1,1} & b_{1,2} \\ b_{2,0} & b_{2,1} & b_{2,2} \end{pmatrix} & a_{1,1} \cdot \begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} \\ b_{1,0} & b_{1,1} & b_{1,2} \\ b_{2,0} & b_{2,1} & b_{2,2} \end{pmatrix} \end{pmatrix} \tag{60}$$

The resulting 6-by-6 matrix is left as a (boring) exercise to the reader.

If A acts on V and B acts on V', then we define the action on their tensor product as:

$$(A \otimes B) * (V \otimes V') = A * V \otimes B * V' \tag{61}$$

What we have learned 2.6. In this section we have introduced the tensor product and how it can be used to **represent a quantum system engulfing two quantum subsystems**. In particular:

- We saw that for an **entangled vector**, since we cannot represent it by a single tensor of two vector but rather as a non trivial sum of tensors, if we know the value of one of those vectors, **we can infer** the value of the other. When those two vectors are a couple of entangled particles, we can then instantly infer the quantum state of one particle from only observing the other particle, even if the two particles are light-years apart.
- Not all systems are entangled, in the case when we cannot infer the state of the second subsystem by measuring the first subsystem, meaning the global system can be expressed as a single tensor, the system is then called **separable**.

3 Exercise Corrections

3.1 Complex Numbers

3.1.1 Exercise 1.1

$$\begin{aligned} c_1 \times c_2 &= (3, -2) \times (1, 2) \\ &= (3 \times 1 - (-2) \times 2, -2 \times 1 + 2 \times 3) \\ &= (3 + 4, -2 + 6) = (7, 4) = 7 + 4i \end{aligned}$$

3.1.2 Exercise 1.2

In this case $a_1 = -2$, $b_1 = 1$, $a_2 = 1$, and $b_2 = 2$. Therefore,

$$\begin{aligned} \frac{-2+i}{1+2i} &= \frac{-2 \times 1 + 1 \times 2}{1^2 + 2^2} + \frac{1 \times 1 - (-2) \times 2}{1^2 + 2^2} \times i \\ &= \frac{0}{5} + \frac{5}{5} \times i = (\frac{0}{5}, \frac{5}{5}) = (0, 1) = i \end{aligned}$$

3.2 Complex Vector Spaces

3.2.1 Exercise 2.1

We need to show that $P * P^{\dagger} = I_3$.

$$P * P^{\dagger} = P * P^{T} = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} * \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Since $\cos\theta^2 + \sin\theta^2 = 1$ we obtain

$$= \begin{pmatrix} \cos\theta\cos\theta - \sin\theta(-\sin\theta) & \cos\theta\sin\theta - \sin\theta\cos\theta & 0 \\ \sin\theta\cos\theta + \cos\theta(-\sin\theta) & \sin\theta\sin\theta + \cos\theta cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} \cos\theta^2 + \sin\theta^2 & 0 & 0 \\ 0 & \cos\theta^2 + \sin\theta^2 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3$$