Math. for Quantum Computing -Linear Algebra-

Linear Algebra provides the mathematical foundations for formulating principles and other results in Quantum Mechanics. We will be reviewed fundamental concepts such as:

- Abstract vector spaces: definition, examples. Linear combinations and linear (in)dependence. Bases. Coordinate vectors.
- Abstract vector inner product. Orthonormal bases
- Linear Transformations. Eigenvectors and eigenvalues. Unitary transformations and matrices. Quantum gates.
- Kroneker product. Tensor product of vector spaces.

This course is based on:

Basic Quantum Knowledge, RoNaQCI, 2024
Advanced Linear and Matrix Algebra, N. Johnston, Springer 2021
Quantum Computing Explained, David McMahon, Wiley-Interscience, 2007

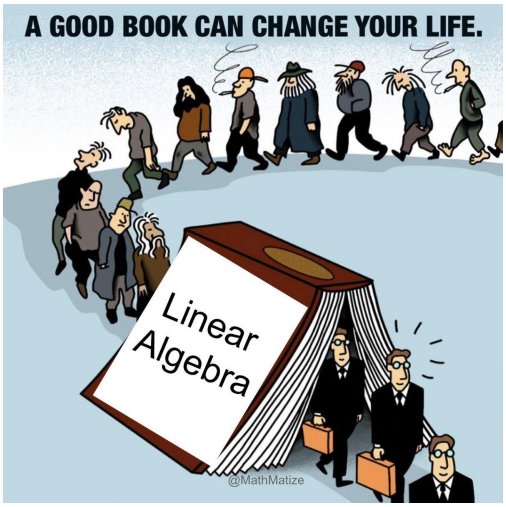


Figure 2.1: Souce: X platform

Short introduction: motivation for studying linear algebra

A quantum circuit diagram generally looks like the following:

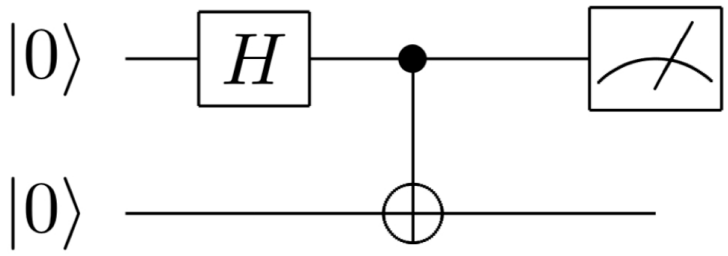
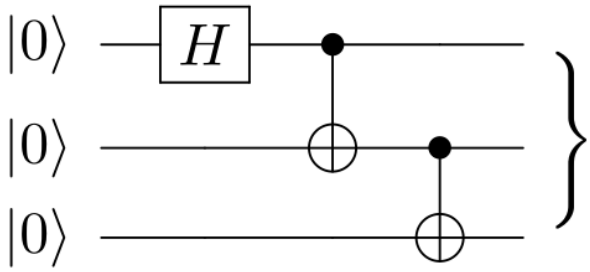


Figure 2.2: Quantum circuit diagram (Wikipedia source)

The main components of a quantum circuit are:

- **Quantum bits**: Each horizontal line in the schematic corresponds to one qubit.
- **Quantum gates**: The boxes and vertical lines in the schematic represent quantum gates. In general, an n-qubit gate is represented by a box spanning the n-qubits (horizontal lines) on which the gate acts.



max. entg. state (see for more last page)

Figure 2.3: Generation of the 3-qubit GHZ state using quantum logic gates.(Wikipedia source)

$I\,|000\rangle \xrightarrow{H_I} (H|0\rangle)|00\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|00\rangle$

$\xrightarrow{(1,2)\ CNOT} = \frac{1}{\sqrt{2}}(|000\rangle + |100\rangle)$

$\xrightarrow{(2,3)\ CNOT} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$

Basic and (more) advanced linear algebra

Vector spaces over $\mathbb{C}$

Quantum objects have a dual character, wave and particle. To describe the wave aspect, one needs two real scalars, an amplitude and an angle, which can be condensed into a single complex number. In QC we work with complex vector spaces.

Let's recall the definition of vector spaces.

Definition 2.1 — Vector Space

Let $\mathcal{V}$ be a set and let $\mathbb{F}(=\mathbb{R}/\mathbb{C})$ be a field. Let $\mathbf{v}, \mathbf{w} \in \mathcal{V}$ and $c \in \mathbb{F}$, and suppose we have defined two operations called *addition* and *scalar multiplication* on $\mathcal{V}$. We write the addition of $\mathbf{v}$ and $\mathbf{w}$ as $\mathbf{v}+\mathbf{w}$, and the scalar multiplication of c and $\mathbf{v}$ as $c\mathbf{v}$.

If the following ten conditions hold for all $\mathbf{v}, \mathbf{w}, \mathbf{x} \in \mathcal{V}$ and all $c, d \in \mathbb{F}$, then $\mathcal{V}$ is called a **vector space** and its elements are called **vectors**:

a) $\mathbf{v}+\mathbf{w} \in \mathcal{V}$ (closure under addition)

b) $\mathbf{v}+\mathbf{w} = \mathbf{w}+\mathbf{v}$ (commutativity)

c) $(\mathbf{v}+\mathbf{w})+\mathbf{x} = \mathbf{v}+(\mathbf{w}+\mathbf{x})$ (associativity)

d) There exists a "zero vector" $\mathbf{0} \in \mathcal{V}$ such that $\mathbf{v}+\mathbf{0} = \mathbf{v}$.

e) There exists a vector $-\mathbf{v}$ such that $\mathbf{v}+(-\mathbf{v}) = \mathbf{0}$.

f) $c\mathbf{v} \in \mathcal{V}$ (closure under scalar multiplication)

g) $c(\mathbf{v}+\mathbf{w}) = c\mathbf{v}+c\mathbf{w}$ (distributivity)

h) $(c+d)\mathbf{v} = c\mathbf{v}+d\mathbf{v}$ (distributivity)

i) $c(d\mathbf{v}) = (cd)\mathbf{v}$

j) $1\mathbf{v} = \mathbf{v}$

?! Lucram cu nr. complexe !?

Example. $\mathbb{C}^n = \left\{ v = \begin{pmatrix} v_0 \\ v_2 \\ \vdots \\ v_{n-1} \end{pmatrix}, v_i \in \mathbb{C} \right\}$ *is a vector space.*

$\mathbb{C}^2 = \{ v = \begin{pmatrix} v_0 \\ v_1 \end{pmatrix}, v_0, v_1 \in \mathbb{C} \}$

- adunarea
- înmulțirea cu scalar $\alpha \cdot v$, $\alpha \in \mathbb{C}$

(Dirac Notation): In Quantum Physics the state of a quantum system is described by a unit vector v, which is usually denoted as $|v\rangle$, called a **ket-vector**.

It can be also associated the **bra-vector** $\langle v| = (\overline{v})^T$, which is also referred as the dual or dagger of $(v^\dagger)$ and it is obtained by performing both complex conjugation and transposition.

Example.

$|v\rangle = \begin{pmatrix} 1+i \\ i \end{pmatrix} \in \mathbb{C}^2$

$\langle v| = (1-i \quad -i)$

Not

$v^+ \equiv v^*$

? 2 operații de făcut : conjugarea + transp.

Example. $\mathcal{M}_{m,n}(\mathbb{C})$, *the set of all* $m \times n$ *matrices with entries from* $\mathbb{C}$, *is a vector space.*

$\mathcal{M}_2 = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{C} \}$

For any matrix $A \in \mathcal{M}_{m,n}(\mathbb{C})$, the following can be associated:

– transpose: A^T, where $A^T[i,j] = A[j,i]$;

– conjugate $\overline{A}$, where $\overline{A}[i,j] = \overline{A[i,j]}$;
– conjugate transpose: $A^\dagger \equiv A^*$, where $A^\dagger[i,j] = \overline{A[j,i]}$.

Example.

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow A^\dagger = A^* = \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix}$$

$z = 1 + i \longrightarrow \overline{z} = 1 - i$

Spans, Linear Combinations, and Independence

We now present some definitions that you likely saw (restricted to $\mathbb{R}^n$) in your first linear algebra course. All of the theorems and proofs involving these definitions carry over just fine when replacing $\mathbb{R}^n$ by a general vector space $\mathcal{V}$, over $\mathbb{C}$.

Definition 2.2 — Linear Combinations

Let $\mathcal{V}$ be a vector space over the field $\mathbb{F}$, let $|v_1\rangle, |v_2\rangle, \ldots, |v_k\rangle \in \mathcal{V}$, and let $c_1, c_2, \ldots, c_k \in \mathbb{C}$. Then every vector of the form

$$c_1|v_1\rangle + c_2|v_2\rangle + \cdots + c_k|v_k\rangle$$

is called a **linear combination** of $|v_1\rangle, |v_2\rangle, \ldots, |v_k\rangle$.

Example. *Is* $|v\rangle = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$ *a linear combination of* $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ *and* $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ *?*

$|v\rangle = 3|0\rangle + 2\cdot|1\rangle$.

Example. *Is* $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *a linear combination of* $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ *and* $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$*?*

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = a\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + b\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + c\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$c = 1$ ✗.

$c = -1$

Definition 2.3 — Span

Let $\mathcal{V}$ be a vector space and let $B \subseteq \mathcal{V}$ be a set of vectors. Then the **span** of B, denoted by $\text{span}(B)$, is the set of all (finite!) linear combinations of vectors from B:

$$\text{span}(B) \stackrel{\text{def}}{=} \left\{ \sum_{j=1}^{k} c_j |v_j\rangle \;\middle|\; k \in \mathbb{N},\ c_j \in \mathbb{F} \text{ and } |v_j\rangle \in B \text{ for all } 1 \leq j \leq k \right\}.$$

Furthermore, if $\text{span}(B) = \mathcal{V}$ then $\mathcal{V}$ is said to be **spanned** by B.

Example. *Let* $E_{i,j}$ *be the matrix with a* 1 *in its* (i,j)*-entry and zeros elsewhere. Show that* $\mathcal{M}_2$ *is spanned by* $E_{1,1}, E_{1,2}, E_{2,1}$*, and* $E_{2,2}$*.*

$$E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

$$E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a\,E_{11} + b\,E_{12} + c\,E_{21} + d\,E_{22}.$$

Definition 2.4 — Linear Dependence and Independence

Let $\mathcal{V}$ be a vector space and let $S \subseteq \mathcal{V}$ be a set of vectors. Then S is **linearly dependent** if there exist scalars $c_1, c_2, \ldots, c_k \in \mathbb{F}$, at

least one of which is not zero, and vectors $|v_1\rangle$, $|v_2\rangle$, ..., $|v_k\rangle \in S$ such that

$$c_1|v_1\rangle + c_2|v_2\rangle + \cdots + c_k|v_k\rangle = \mathbf{0}.$$

If S is not linearly dependent then it is called **linearly independent**.

A spanning set for qubits $|\varphi\rangle \in \mathbb{C}^2$ can be found using the vectors $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ and $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$ as, due to superposition, we have that

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle, \forall \alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1.$$

com. lmană ; $\mathbb{C}^2$

Definition 2.5 — Bases

A **basis** of a vector space $\mathcal{V}$ is a set of vectors in $\mathcal{V}$ that

a) spans $\mathcal{V}$, and

b) is linearly independent.

Be careful: A vector space can have many bases that look very different from each other!

Example. *Let $\mathbf{e}_j$ be the vector in $\mathbb{R}^n$ with a 1 in its j-th entry and zeros elsewhere. Show that $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$ is a basis of $\mathbb{R}^n$.*

*[Side note: This is called the **standard (computational) basis** of $\mathbb{R}^n$.]*

$\mathbb{C}^2$: $B_C = \{ |0\rangle \equiv \begin{pmatrix}1\\0\end{pmatrix} ; |1\rangle \equiv \begin{pmatrix}0\\1\end{pmatrix} \}$

$|0\rangle = e_1$ $|1\rangle = e_2$

Example. ***Hadamard basis*** *of $\mathbb{C}^2$ is $B_H = \{h_1, h_2\}$, where $|h_1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ and $|h_2\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$.*

$|h_1\rangle = |+\rangle$ $|h_2\rangle = |-\rangle$

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$$

$$|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$$?

Example. *Let $E_{i,j} \in \mathcal{M}_{m,n}$ be the matrix with a 1 in its (i,j)-entry and zeros elsewhere. Show that $\{E_{1,1}, E_{1,2}, \ldots, E_{m,n}\}$ is a basis of $\mathcal{M}_{m,n}$. [Side note: This is called the **standard basis** of $\mathcal{M}_{m,n}$.]*

$B = \{E_{ij}\}_{i,j}$

Example. *Is the set $B = \{I, X, Y, Z\}$ (introduced before) a basis of $\mathcal{M}_2(\mathbb{C})$?*

Pauli matrices ?

Definition 2.6 — Coordinate Vectors

Suppose $\mathcal{V}$ is a vector space over a field $\mathbb{F}$ with a finite (ordered) basis $B = \{|v_1\rangle, |v_2\rangle, \ldots, |v_n\rangle\}$, and $|v\rangle \in \mathcal{V}$. Then the unique scalars c_1, c_2, …, $c_n \in \mathbb{F}$ for which

$$|v\rangle = c_1|v_1\rangle + c_2|v_2\rangle + \cdots + c_n|v_n\rangle$$

are called the **coordinates** of $|v\rangle$ with respect to B, and the vector

$$[\mathbf{v}]_B \stackrel{\text{def}}{=} (c_1, c_2, \ldots, c_n)^T$$

is called the **coordinate vector** of **v** with respect to B.

Example. *Find the coordinate of the vectors of Hadamard basis*

$$\mathcal{B}_H = \{|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}\}$$

respect to computational basis

$$B_c = \{|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}, |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}\}.$$

.

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1\\0\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix}\right] = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$

$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ $\qquad [|+\rangle]_{B_c} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$

$[|-\rangle]_{B_c} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$

Definition 2.7 — Dimension of a Vector Space

A vector space $\mathcal{V}$ is called...

a) **finite-dimensional** if it has a finite basis, and its **dimension**, denoted by $\dim(\mathcal{V})$, is the number of vectors in one of its bases.

b) **infinite-dimensional** if it has no finite basis, and we say that $\dim(\mathcal{V}) = \infty$.

Example. *Let's compute the dimension of some vector spaces that we've been working with.*

$\dim(\mathbb{C}^2) = 2$, $\dim(\mathbb{C}^n) = n$

$\dim(\mathcal{M}_{m,n}) = m \cdot n$

Change of Basis

Sometimes one basis (i.e., coordinate system) will be much easier to work with than another. While it is true that the standard basis (of $\mathbb{R}^n$, $\mathbb{C}^n$, or $\mathcal{M}_{m,n}$) is often the simplest one to use for calculations, other bases often reveal hidden structure that can make our lives easier.

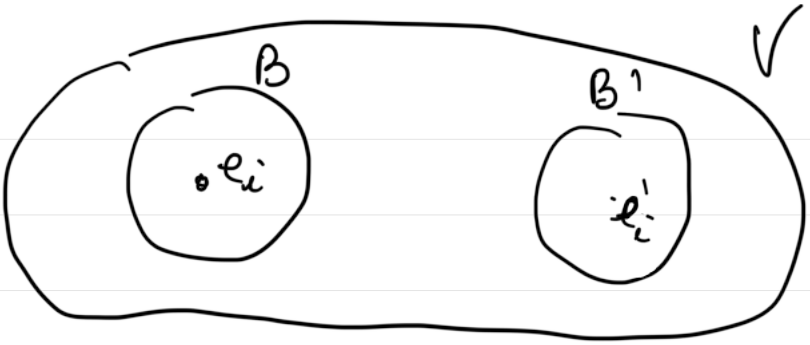
We will discuss how to find these other bases shortly, but for now let's talk about how to convert coordinate systems from one basis to another.

Definition 2.8 — Change-of-Basis Matrix

Suppose $\mathcal{V}$ is a vector space with bases $B = \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$ and $B' = \{\mathbf{e}'_1, \mathbf{e}'_2, \ldots, \mathbf{e}'_n\}$. The **change-of-basis matrix** from B to B', denoted by $T_{B' \leftarrow B}$, is the matrix

$$T_{B' \leftarrow B} = (t_{ij})$$

where $e'_j = \sum_i t_{ij} e_i$.



The following theorem shows that the change-of-basis matrix $T_{B' \leftarrow B}$ does exactly what its name suggests: it converts coordinate vectors from basis B to basis C.

Theorem 2.1 — Change-of-Basis Matrices

Suppose B and B' are bases of a finite-dimensional vector space $\mathcal{V}$, and let $P_{B' \leftarrow B}$ be the change-of-basis matrix from B to B'. Then

a) $T_{B' \leftarrow B}[\mathbf{v}]_B = [\mathbf{v}]_{B'}$ for all $\mathbf{v} \in \mathcal{V}$, and

b) $T_{B' \leftarrow B}$ is invertible and $T^{-1}_{B' \leftarrow B} = T_{B \leftarrow B'}$.

Furthermore, $T_{B' \leftarrow B}$ is the unique matrix with property (a).

Example. *Find the change of basis from the computational basis* $B_c = \{|0\rangle, |1\rangle\} \subset \mathbb{C}^2$ *to the Hadamard basis* $B_H = \{|\pm\rangle\} \subset \mathbb{C}^2$.

$$T_{B_C B_H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \equiv H.$$

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$|-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Abstract Vector Inner Products, Orthonormal Bases

Definition 2.9 — Inner Product (IP)

Suppose that $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$, and $\mathcal{V}$ is a vector space over $\mathbb{F}$. Then an **inner product** on $\mathcal{V}$ is a function $\langle \cdot, \cdot \rangle : \mathcal{V} \times \mathcal{V} \to \mathbb{F}$ such that the following three properties hold for all $c \in \mathbb{F}$ and all $\mathbf{v}, \mathbf{w}, \mathbf{x} \in \mathcal{V}$:

a) $\langle \mathbf{v}, \mathbf{w} \rangle = \overline{\langle \mathbf{w}, \mathbf{v} \rangle}$ (conjugate symmetry)

b) $\langle \mathbf{v}, \mathbf{w} + c\mathbf{x} \rangle = \langle \mathbf{v}, \mathbf{w} \rangle + c\langle \mathbf{v}, \mathbf{x} \rangle$ (linearity in 2nd entry)

c) $\langle \mathbf{v}, \mathbf{v} \rangle \geq 0$, with equality if and only if $\mathbf{v} = \mathbf{0}$. (positive definiteness)

Inner products are *not* linear in their first argument.

Example. *Standard (Euclidian) IP on* $\mathbb{C}^n$*:*

$$\langle \mathbf{v}, \mathbf{w} \rangle = \mathbf{v}^\dagger |\mathbf{w}\rangle = \sum_{i=1}^{n} \overline{v_i} w_i \quad \textit{for all} \quad \mathbf{v}, \mathbf{w} \in \mathbb{C}^n.$$

$$= \begin{pmatrix} \overline{v_1} & \overline{v_2} \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$$

$v = \begin{pmatrix} 1 \\ i \end{pmatrix}$, $w = \begin{pmatrix} 1+i \\ 2 \end{pmatrix}$

$\langle v, w \rangle = \underbrace{(1 \quad -i)}_{v^+} \begin{pmatrix} 1+i \\ 2 \end{pmatrix} = 1+i-2i = 1-i$

$\langle v| = v^+$ bra , $|w\rangle = w$ ket

Example. *Show that the following function is an inner product on* $\mathcal{M}_{m,n}$*:*

$$\langle A, B \rangle = \operatorname{tr}(A^\dagger B) \quad \textit{for all} \quad A, B \in \mathcal{M}_{m,n}.$$

This inner product is typically called the ***Frobenius inner product*** *or* ***Hilbert–Schmidt inner product****.*

A vector space together with a particular inner product is called an **inner product space**.

> If $A \in \mathcal{M}_{m,n}(\mathbb{C})$ and v, w are column vectors, then IP $< v|A \cdot w >$ can be denoted as $< v|A|w >$. Therefore,
>
> $$< v|A|w > = \overline{v} \cdot (A \cdot w) = (\overline{v} \cdot A) \cdot w = < A^\dagger v|w >$$

Example. *Compute* $\underbrace{< 0|A|0 >}_{a}$, $\underbrace{< 0|A|1 >}_{b}$, $\underbrace{< 1|A|0 >}_{c}$ *and* $\underbrace{< 1|A|1 >}_{d}$, *for* $A \in \mathcal{M}_2(\mathbb{C})$.

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightsquigarrow \langle 0|A|0\rangle = (1 \; 0)\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$= (a \quad b)\begin{pmatrix} 1 \\ 0 \end{pmatrix} = a$

$\langle 0|A|1\rangle = (1 \; 0)\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = b$

$$A = \begin{pmatrix} \langle 0|A|0\rangle & \langle 0|A|1\rangle \\ \langle 1|A|0\rangle & \langle 1|A|1\rangle \end{pmatrix}.$$

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$\langle\varphi|\varphi\rangle = \begin{pmatrix} \bar{\alpha} & \bar{\beta} \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha\bar{\alpha} + \beta\bar{\beta} = |\alpha|^2 + |\beta|^2$$

$$\||\varphi\rangle\| = \sqrt{\langle\varphi|\varphi\rangle} = 1 \Rightarrow |\alpha|^2 + |\beta|^2 = 1$$

Definition 2.10 — Norm Induced by the Inner Product

Suppose that $\mathcal{V}$ is an inner product space. Then the **norm induced by the inner product** is the function $\|\cdot\| : \mathcal{V} \to \mathbb{R}$ defined by

$$\|\mathbf{v}\| \stackrel{\text{def}}{=} \sqrt{\langle \mathbf{v}, \mathbf{v}\rangle} \quad \text{for all} \quad \mathbf{v} \in \mathcal{V}.$$

Example. *What is the norm induced by the standard inner product on* $\mathbb{C}^n$*?*

Example. *What is the norm induced by the standard (Frobenius) inner product on* $\mathcal{M}_{m,n}$*?*

A quantum state $|\varphi\rangle$ is said to be **normalized quantum state** if its norm is equal to 1(it is a unit vector):

$$\||\varphi\rangle\| = 1$$

For a qubit in a superposition state $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$, the normalization condition becomes $|\alpha|^2 + |\beta|^2 = 1$.

Example. *Check if the state* *is normalized.*

Definition 2.11 — Orthogonality

Suppose $\mathcal{V}$ is an inner product space. Then two vectors $\mathbf{v}, \mathbf{w} \in \mathcal{V}$ are called **orthogonal** if $\langle \mathbf{v}, \mathbf{w} \rangle = 0$.

Definition 2.12 — Orthonormal Bases

A basis B of an inner product space $\mathcal{V}$ is called an **orthonormal basis** of $\mathcal{V}$ if

a) $\langle \mathbf{v}, \mathbf{w} \rangle = 0$ for all $\mathbf{v} \neq \mathbf{w} \in B$, and (mutual orthogonality)

b) $\|\mathbf{v}\| = 1$ for all $\mathbf{v} \in B$. (normalization)

Example. *Examples of orthonormal bases in our "standard" vector spaces include:*

$B_C = \{|0\rangle, |1\rangle\}$

$B_H = \{|+\rangle, |-\rangle\}$

$\langle +|+\rangle = 1 \quad \langle +|-\rangle = 0$

$\langle -|-\rangle = 1 \quad \langle -|+\rangle = 0$

$\langle 0|0\rangle = 1$

$\langle 0|1\rangle = 0$

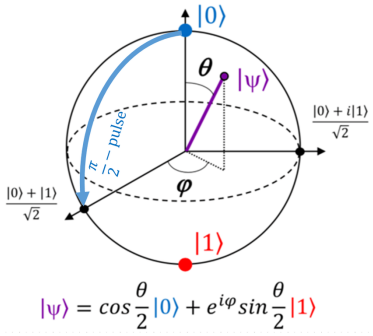
$\langle 1|0\rangle = 0$

$\langle 1|1\rangle = 1$

$e^{i\theta} \equiv \cos\theta + i\sin\theta$

Bloch sphere representation

Given a qubit in the state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, with $|\alpha|^2 + |\beta|^2 = 1$, the complex parameters α and β can be represented as $\alpha = r_0 e^{i\varphi_0}$ and $\beta = r_1 e^{i\varphi_2}$. Consequently, $|\Psi\rangle = r_0|0\rangle + r_1 e^{i\varphi}|1\rangle$, where $\varphi = \varphi_1 - \varphi_0 \in [0, 2\pi)$. As $|r_0|^2 + |r_1|^2 = 1$, we could interpret that $r_0 = \cos(\theta/2)$ and $r_1 = \sin(\theta/2)$, where $\theta \in [0, \pi]$. Therefore, a single qubit $|\Psi\rangle$ can be



expressed in a geometrical way using, what is called, **Bloch sphere**.

$$|\Psi\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)e^{i\varphi}|1\rangle$$

Bloch sphere is a geometrical representation of a single qubit as a point on 3-D sphere of radius 1, where $(1; \theta, \varphi)-$ Bloch vector of $|\Psi\rangle$:

- θ and φ are real numbers representing the polar and azimuthal angles
- the north pole corresponds to the state $|0\rangle$
- the south pole corresponds to the state $|1\rangle$

The Bloch sphere gives an intuitive way to visualize qubit states and the transformations that act upon them, such as quantum gates.

Linear Transformation

Definition 2.13 — Linear Transformations

Let $\mathcal{V}$ and $\mathcal{W}$ be vector spaces over the same field $\mathbb{F}$. A **linear transformation** is a function $\mathcal{T} : \mathcal{V} \to \mathcal{W}$ that satisfies the following two properties:

a) $\mathcal{T}(|v\rangle + |w\rangle) = \mathcal{T}(|v\rangle) + \mathcal{T}(|w\rangle)$ for all $|v\rangle, |w\rangle \in |V\rangle$, and

b) $\mathcal{T}(c|v\rangle) = c\mathcal{T}(|v\rangle)$ for all $|v\rangle \in \mathcal{V}$ and $c \in \mathbb{F}$.

We will write $\mathcal{T}|v\rangle$ instead of $\mathcal{T}(|v\rangle)$.
If $\mathcal{T} : \mathcal{V} \to \mathcal{W}$ and $\mathcal{S} : \mathcal{W} \to$, then $\mathcal{S} \circ \mathcal{T}$ (also denoted as $\mathcal{ST}$) is also a linear transformation and $(\mathcal{ST})|v\rangle = \mathcal{S}(\mathcal{T}|v\rangle)$.

Example. *Every matrix transformation is a linear transformation. That is, if $A \in \mathcal{M}_{m,n}$ then $\mathcal{T}_A : \mathbb{R}^n \to \mathbb{R}^m$, defined by $\mathcal{T}_A(v) = Av$, is a linear*

transformation.

Theorem 2.2 — Standard Matrix of a Linear Transformation

Let $\mathcal{V}$ and $\mathcal{W}$ be vector spaces with bases $B = \{|v_i\rangle\}_{i=1}^n$ and $B' = \{|w_j\rangle\}_{j=1}^m$. A function $\mathcal{T} : \mathcal{V} \to \mathcal{W}$ is a linear transformation if and only if there exists a matrix $[\mathcal{T}]_{B' \leftarrow B} \in \mathcal{M}_{m,n}$ for which

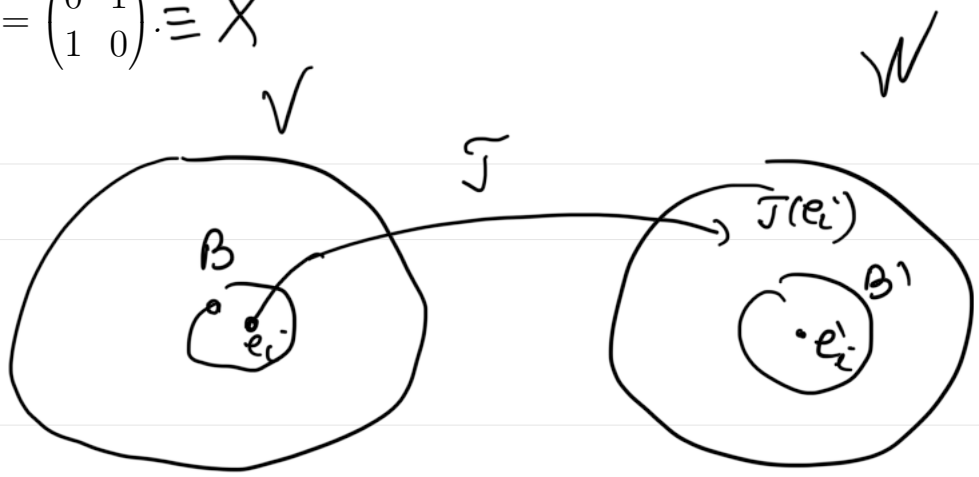
$$[\mathcal{T}(\mathbf{v})]_{B'} = [\mathcal{T}]_{B' \leftarrow B}[|v\rangle]_B \quad \text{for all} \quad |v\rangle \in \mathcal{V}.$$

Furthermore, the unique matrix $[\mathcal{T}]_{B' \leftarrow B}$ with this property is called the **standard matrix** of $\mathcal{T}$ with respect to the bases B and B', and it is

$$[\mathcal{T}]_{B' \leftarrow B} \stackrel{\text{def}}{=} \Big[\ [\mathcal{T}|v_1\rangle]_{B'} \ \Big|\ [\mathcal{T}|v_2\rangle]_{B'} \ \Big|\ \cdots \ \Big|\ [\mathcal{T}|v_n\rangle]_{B'}\ \Big].$$

In the bases $B = B'$, then we write $[\mathcal{T}]_{B \leftarrow B} = [\mathcal{T}]_B$.

Example. *Let* $\mathcal{V} = \mathbb{C}^2$ *and* $B = \{|0\rangle, |1\rangle\}$ *and* $\mathcal{A} : \mathcal{V} \to \mathcal{V}$, *such that* $\mathcal{A}|0\rangle = |1\rangle$ *and* $\mathcal{A}|1\rangle = |0\rangle$. *The standard matrix associated to basis* B *is* $[\mathcal{A}]_B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.



Example. *If a matrix $A \in \mathcal{M}_{m,n}(\mathbb{C})$ is associated to the linear transformation*

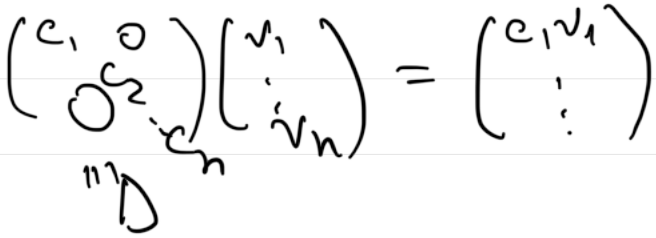
$$\mathcal{T}_A : \mathbb{C}^n \to \mathbb{C}^m, \text{ defined by } \mathcal{T}_A|v\rangle = A|v\rangle,$$

then the matrix associate to $\mathcal{T}_A$ relative to the computational basis $B = \{e_i\}_i$ is precisely A.

A Catalog of Linear Transformations

Example. ***The zero and identity transformations.***
Zero transformation *$O : \mathbb{R}^n \to \mathbb{R}^m$, defined by $O(\mathbf{v}) = \mathbf{0}$ for all $\mathbf{v} \in \mathbb{R}^n$.*
Identity transformation *$I : \mathbb{R}^n \to \mathbb{R}^n$, defined by $I(\mathbf{v}) = \mathbf{v}$ for all $\mathbf{v} \in \mathbb{R}^n$.*

Example. ***Diagonal transformations/matrices.***
$T : \mathbb{R}^n \to \mathbb{R}^n$, $T(v_1, v_2, \ldots, v_n)^T = (c_1 v_1, c_2 v_2, \ldots, c_n v_n)^T$.
It does not change the direction of the standard basis vectors, but simply stretches them by certain amounts (possibly different).



Example. ***Projection onto the x/y-axis.***
Function that sends (v1,v2) to (v1,0)

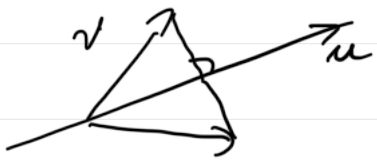
Example. ***Projection onto a line***, *$P_{\mathbf{u}} : \mathbb{R}^n \to \mathbb{R}^n$.*
$P_u(v) = \|\mathbf{v}\| \cos(\theta)\mathbf{u} = (uu^T)v$.

Example. ***Rotation*** $R^\theta : \mathbb{R}^2 \to \mathbb{R}^2$ *counter-clockwise around the origin by an angle of* θ.
Here, $[R^\theta] = \begin{pmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{pmatrix}$.

Example. *Reflection of a vector* $\mathbf{v}$ *across the line in the direction of* $\mathbf{u}$. *By the transformation* $F_{\mathbf{u}} : \mathbb{R}^n \to \mathbb{R}^n$ *we aim to reflect the space through the line in the direction of the unit vector* $\mathbf{u}$.
We have that

$$F_{\mathbf{u}}(\mathbf{v}) = \mathbf{v} + 2(P_{\mathbf{u}}(v) - \mathbf{v}) = (2\mathbf{u}\mathbf{u}^T - I)\mathbf{v}$$

The standard matrix of the reflection transformation is $[F_{\mathbf{u}}] = 2\mathbf{u}\mathbf{u}^T - I$.



Definition 2.14

If $\mathcal{V}$ and $\mathcal{W}$ are two linear spaces endowed with the inner products, then for any fixed vectors $v \in \mathcal{V}$ and $w \in \mathcal{W}$, we can defined the linear map

$$f : \mathcal{V} \to \mathcal{V},\ f(u) = \langle v|u\rangle w,$$

called the outer product of the vectors v and w, denoted as $|w\rangle\langle v|$.

The **outer product** of a ket $|\varphi\rangle$ and a bra $\langle\phi|$, which is written as $|\varphi\rangle\langle\phi|$, is an operator(a transformation). It acts as follows:

ket bra

$$(|\varphi\rangle\langle\phi|)|a\rangle = |\varphi\rangle\langle\phi|a\rangle = (\langle\phi|a\rangle)|\varphi\rangle$$

It can be seen that the bra-ket transformation transforms the vector $|a\rangle$ into one proportional to $|\varphi\rangle$; the number $\langle\phi|a\rangle$ is the constant of proportionality.

Let's examine the outer product using matrices. If $|\varphi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ and $|\phi\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$, then the outer product is

ket bra

$$|\varphi\rangle\langle\phi| = \begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} \bar{c} & \bar{d} \end{pmatrix} = \begin{pmatrix} a\bar{c} & a\bar{d} \\ b\bar{c} & b\bar{d} \end{pmatrix}$$

$|u\rangle\langle v|$ ket-bra = matrice = outer product

$\langle u|v\rangle$ bra-ket = scalar = inner product.

Completeness relation If $I : \mathcal{V} \to \mathcal{V}$ is the identity operator on $\mathcal{V}$, i.e. $I(v) = v$, $\forall v \in \mathcal{V}$, then it can be written as

$$I = \sum_i |e_i\rangle\langle e_i|,$$

where $B = \{e_i\}$ is an orthonormal basis in $\mathcal{V}$.

$I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}(1\ 0) + (0\ 1)\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$= \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}}_{E_{11}} + \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{E_{22}} = I$ ✓.

The projection operator onto the direction of the unit vector e_i can

Temă: $I = |+\rangle\langle+| + |-\rangle\langle-|$

be defined as

$$P_i : \mathcal{V} \to \mathcal{V},\ u \mapsto u_i e_i = \langle e_i|u\rangle e_i$$

Therefore, $P_i(u) = \langle e_i|u\rangle e_i = |e_i\rangle\langle e_i|(u)$, so $P_i = |e_i\rangle\langle e_i|$.

Using the completeness relation, we can write $\mathcal{A} = I_W \circ \mathcal{A} \circ I_V$. Therefore, the representation of operator $\mathcal{A}$ using the outer product is

$A = a E_{00} + b E_{01} + c E_{10} + d E_{11}$

$|0\rangle\langle 0|$ $|0\rangle\langle 1|$ $|1\rangle\langle 0|$ $|1\rangle\langle 1|$

$$\mathcal{A} = \sum_{i,j} a_{ij} |w_i\rangle\langle v_j|$$

Here the element a_{ij} of the matrix A is $a_{ij} =< w_i|A|v_j >$.

For operators that act on qubits, we represent the operator by 2×2 matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = a|0\rangle\langle 0| + b|0\rangle\langle 1| + c|1\rangle\langle 0| + d|1\rangle\langle 1|$.

In a simple manner, we can find the adjoint (conjugate transpose of A), using the fact that $(|u\rangle\langle v|)^\dagger = |v\rangle\langle u|$. Therefore, $(|0\rangle\langle 0|)^\dagger = |0\rangle\langle 0|$, $(|1\rangle\langle 0|)^\dagger = |0\rangle\langle 1|$

$$A^\dagger = \overline{a}|0\rangle\langle 0| + \overline{b}|1\rangle\langle 0| + \overline{c}|0\rangle\langle 1| + \overline{d}|1\rangle\langle 1| = \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix}.$$

The matrix representation of an operator with respect to the computational basis $B_c = \{|0\rangle, |1\rangle\} \subset \mathbb{C}^2$ is

$$A = \begin{pmatrix} < 0|A|0 > & < 0|A|1 > \\ < 1|A|0 > & < 1|A|1 > \end{pmatrix}.$$

Moreover, $Tr(A) = \sum\limits_i < i|A|i >$.

Example. *Write the Pauli matrices as outer products and find their adjoint matrix.*

$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 1 \cdot |0\rangle\langle 1| + 1 \cdot |1\rangle\langle 0|$

$X^\dagger = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = (|0\rangle\langle 1| + |1\rangle\langle 0|)^\dagger =$

$= |1\rangle\langle 0| + |0\rangle\langle 1|. = X$

$\cdot X$ - Hermitiană.

The connection between linear transformation $\mathcal{A}$ and the matrices A is very tight, but non-canonical, in the sense that it depends on the choice/fixing of bases.

Adjoint Transformations

Definition 2.15 — Adjoint Transformations

Suppose that $\mathcal{V}$ and $\mathcal{W}$ are inner product spaces and $T : \mathcal{V} \to \mathcal{W}$ is a linear transformation. Then a linear transformation $T^* : \mathcal{W} \to \mathcal{V}$ is called the **adjoint** of T if

$$\langle T(\mathbf{v}), \mathbf{w} \rangle = \langle \mathbf{v}, T^*(\mathbf{w}) \rangle \quad \text{for all} \quad \mathbf{v} \in \mathcal{V} \text{ and } \mathbf{w} \in \mathcal{W}.$$

For example, the adjoint of a matrix $A \in \mathcal{M}_{m,n}(\mathbb{C})$ is

Definition 2.16 — Self-Adjoint Transformations

Suppose that $\mathcal{V}$ is an inner product space. Then a linear transformation $T : \mathcal{V} \to \mathcal{V}$ is called **self-adjoint** if $T^* = T$.

For example, a matrix in $\mathcal{M}_n(\mathbb{R})$ is self-adjoint if and only if it is symmetric (i.e., $A = A^T$),

and a matrix in $\mathcal{M}_n(\mathbb{C})$ is self-adjoint if and only if it is Hermitian (i.e., $A = A^\dagger \equiv A^*$). Therefore, if $A = (a_{ij}), 1 \leq i, j \leq n$, then A is Hermitian iff $a_{ij} = \overline{a_{ji}}, \forall i, j$.

Furthermore, a linear transformation is self-adjoint if and only if its standard matrix is symmetric/Hermitian (with respect to some orthonormal basis).

$A = A^\dagger$

Eigenvectors and eigenvalues

Definition 2.17

Let $\mathcal{V}$ be a complex linear space of dimension n (in particular $\mathbb{C}^n$ and let $f : \mathcal{V} \to \mathcal{V}$ be a linear operator. A scalar $\lambda \in \mathbb{C}$ is called an eigenvalue of f if there exists a nonzero vector v such that

$$f(v) = \lambda v$$

A vector $v \in \mathcal{V}$ is called an eigenvector of f if $v \neq 0$ and there exists $\lambda \in \mathbb{C}$ such that $f(v) = \lambda v$.

If A is the standard matrix of the operator f respect to the basis B, then $Av = \lambda v$ and the polynomial $P_A(\lambda) = det(A - \lambda I)$ is called the characteristic polynomial of the matrix A. The spectrum of the operator f is the set

$$Spec(f) = \{\lambda_1, \ldots, \lambda_p\},$$

where each eigenvalue λ_i is counted with its algebraic multiplicity $n_i, i = \overline{1,p}$. Hence, $P_f(\lambda) = (-1)^n(\lambda - \lambda_1)^{n_1} \ldots (\lambda - \lambda_p)^{n_p}$, with $n_1 + \ldots + n_p = n$.

Theorem 2.3

The operator f is called diagonalizable if there is a basis B of $\mathcal{V}$ such that the standard matrix is diagonal. It is shown that f is diagonalizable iff $din(V) = n_\lambda$ for any $\lambda \in Spec(f)$, in which case the following decomposition in direct sum of the subspaces holds $V = V(\lambda_1) \oplus \cdots \oplus V(\lambda_p)$. Consequently,

$$f = \sum_i \lambda_i p_i, \text{ where } p_i = |i\rangle\langle i|.$$

This relation is called spectral theorem.

Example. *Use the spectral theorem to write the Pauli matrix Z using the outer product.*

In Quantum Mechanics any physical observables is associated with a Hermitian matrix (or a self-adjoint operator).

This is based on the following property:

Corollary 2.4 — Properties of Hermitian matrices

Given $A \in \mathcal{M}_n(\mathbb{C})$ a Hermitian matrix, then it holds:

a) The eigenvalues of A are real.

b) If λ and λ' are distinct eigenvalues of A, then the corresponding eigenvectors are orthogonal.

Unitary Transformations and Matrices

In situations where the norm of a vector is important, it is often desirable to work with linear transformations that do not alter that norm. We now start investigating these linear transformations.

Definition 2.18 — Unitary Transformations

Let $\mathcal{V}$ and $\mathcal{W}$ be inner product spaces and let $T : \mathcal{V} \to \mathcal{W}$ be a linear transformation. Then T is said to be **unitary** if

$$\|T(\mathbf{v})\| = \|\mathbf{v}\| \quad \text{for all} \quad \mathbf{v} \in \mathcal{V}.$$

Theorem 2.5 — Characterization of Unitary Matrices

Suppose $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$, and $U \in \mathcal{M}_n(\mathbb{F})$. The following are equivalent:

a) U is unitary,

b) $U^\dagger U = I$,

c) $UU^\dagger = I$,

d) $(U\mathbf{v}) \cdot (U\mathbf{w}) = \mathbf{v} \cdot \mathbf{w}$ for all $\mathbf{v}, \mathbf{w} \in \mathbb{F}^n$,

e) The columns of U are an orthonormal basis of $\mathbb{F}^n$, and

f) The rows of U are an orthonormal basis of $\mathbb{F}^n$.

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

$$H \cdot H^\dagger = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = I$$

More generally, every rotation matrix and reflection matrix is unitary, as we now demonstrate.

Example. *Show that every rotation matrix $U \in \mathcal{M}_2(\mathbb{R})$ is unitary. We*

use that

$$U = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$$

for some $\theta \in \mathbb{R}$*, and we compute* $U^\dagger U$*.*

$UU^\dagger = \left(\quad\right)\left(\quad\right) = I$

Corollary 2.6 — Properties of unitary matrices

Given $A \in \mathcal{M}_n(\mathbb{C})$ an unitary matrix, then

a) A preserves the Euclidean inner product.

b) A preserves the Euclidean norm and the measurement of angles.

c) If v is a ket vector, then knowing the transform $v' = Av$, we can directly recover v.

d) The eigenvalues of A have absolute value 1.

Single Qubit Gates

Quantum gates are employed to transport and manipulate quantum information. When applying to a single qubit, they can be represented by a 2×2 matrix; for physical considerations, they have to be also unitary transformations. In the following we present a list of the most used quantum gates:

– **Quantum NOT gate**:

$$X = U_{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$$

Let's see how X acts on the vectors of the computational basis:

$X|0\rangle = (|0\times 1| + |1\times 0|)|0\rangle = 0\times 1|0\rangle + 1\times 0|0\rangle = |1\rangle$

$X|1\rangle = |0\times 1|1\rangle + |1\times 0|1\rangle = |0\rangle$

– **Hadamard gate**:

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

Let's see how H acts on the vectors of the computational basis:

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

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

In general, it can be proved that any 2×2 unitary matrix can be decomposed in a product of rotation matrices. More exactly, if U is an unitary matrix, then there exists four real values $(\alpha, \beta, \gamma, \delta)$ such that U can be written as follows:

$$U = e^{i\alpha}\begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix}\begin{pmatrix} \cos(\gamma/2) & -\sin(\gamma/2) \\ \sin(\gamma/2) & \cos(\gamma/2) \end{pmatrix}\begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix}$$

– **Phase shift gate**:

$$P_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} = |0\rangle\langle 0| + e^{i\alpha}|1\rangle\langle 1|, \forall \alpha \in \mathbb{R}$$

Let's see how P_α acts on:

Moreover, $P_{\pi/2} \equiv S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ or $P_{\pi/4} \equiv T = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{pmatrix}$

Properties of single qubit gates:

- $HXH = Z$
- $HYH = -Y$
- $HZH = X$
- $TT = S$
- $TTTT = Z$
- $H = (X + Z)/\sqrt{2}$.

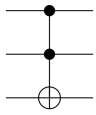
Operator	Gate(s)	Matrix
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Figure 2.4: Common quantum logic gates by name (including abbreviation), circuit form(s) and the corresponding unitary matrices.(Wikipedia source)

Normal Matrices and the Spectral Decomposition

Definition 2.19 — Normal Matrix

A matrix $A \in \mathcal{M}_n(\mathbb{C})$ is called **normal** if $A^*A = AA^*$.

Many of the important families of matrices that we are already familiar with are normal. For example unitary, hermitian, skew-hermitian, diagonal.

Example. *Show that the matrix* $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ *is normal.*

$Y^\dagger = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = Y \implies Y \cdot Y^\dagger = Y^\dagger Y$.

Our primary interest in normal matrices comes from the following theorem, which says that normal matrices are exactly those that can be diagonalized by a unitary matrix:

Theorem 2.7 — Complex Spectral Decomposition

Suppose $A \in \mathcal{M}_n(\mathbb{C})$. Then there exists a unitary matrix $U \in \mathcal{M}_n(\mathbb{C})$ and diagonal matrix $D \in \mathcal{M}_n(\mathbb{C})$ such that

$$A = UDU^\dagger$$

if and only if A is normal (i.e., $A^\dagger A = AA^\dagger$).

We notice that the spectral decomposition is a special case of diagonalization where the invertible matrix that does the diagonalization is unitary, so we compute it via eigenvalues and eigenvectors (like we usually do for diagonalization, via eigenvalues and eigenvectors). Just be careful to choose the eigenvectors to have length 1 and be mutually orthogonal.

We recall that the spectral decomposition of a normal operator A means that the operator has a diagonal matrix representation in a ortonormal basis $\{|e_i\rangle\}_{i=1}^n$ of the form

$$A = \sum_{i=1}^{n} \lambda_i |e_i\rangle\langle e_i|$$

Here λ_i are the eigenvalues of the operator, whereas the vectors $|e_i\rangle$ are the eigenvectors.
For example, the Pauli operator Z can be written $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$.
The spectral decomposition helps to compute **functions of opera-**

tors:

$$\hat{f}(A) = \sum_{i=1}^{n} f(\lambda_i)|e_i\rangle\langle e_i|$$

Example. *Prove that* $e^Z = \begin{pmatrix} e & 0 \\ 0 & 1/e \end{pmatrix}$.

$Z = |0\times 0| - |1\times 1|$ $\quad \lambda = \pm 1$

$e^Z = e^1 |0\times 0| + e^{-1} |1\times 1| = \begin{pmatrix} e^1 & 0 \\ 0 & 1/e \end{pmatrix}$

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

Definition 2.20 — Positive (Semi)Definite Matrices

Suppose $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$, and $A = A^\dagger \in \mathcal{M}_n(\mathbb{F})$. Then A is called

a) **positive semidefinite (PSD)** if $\mathbf{v}^\dagger A\mathbf{v} \geq 0$ for all $\mathbf{v} \in \mathbb{F}^n$, and

b) **positive definite (PD)** if $\mathbf{v}^\dagger A\mathbf{v} > 0$ for all $\mathbf{v} \neq \mathbf{0}$.

Positive (semi)definiteness is somewhat difficult to eyeball from the entries of a matrix, and we should emphasize that it does *not* mean that the entries of the matrix need to be positive. For example, if

$$A = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix},$$

then...

$\begin{vmatrix} 1-\lambda & -1 \\ -1 & 1-\lambda \end{vmatrix} = (1-\lambda)^2 - 1 = 0 \to 0$

$1-\lambda = -1$

$\to 2 \to 0 \to$ P.S.D.

The next theorem characterizes these matrices in several other equivalent ways, some of which are hopefully a bit more illuminating and easier to work with.

Theorem 2.8 — Characterization of PSD and PD Matrices

Suppose $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$, and $A = A^* \in \mathcal{M}_n(\mathbb{F})$. The following are equivalent:

a) A is positive (semidefinite | definite),

b) All of the eigenvalues of A are (non-negative | strictly positive),

c) There exists a diagonal $D \in \mathcal{M}_n(\mathbb{R})$ with (non-negative | strictly positive) diagonal entries and a unitary matrix $U \in \mathcal{M}_n(\mathbb{F})$ such that $A = UDU^*$, and

d) There exists (a matrix | an invertible matrix) $B \in \mathcal{M}_n(\mathbb{F})$ such that $A = B^*B$.

The Kroneker Product

Definition 2.21 — Kroneker product

The **Kronecker product** of matrices $A \in \mathcal{M}_{m,n}$ and $B \in \mathcal{M}_{p,q}$ is the block matrix

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \dots & \vdots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{pmatrix} \in \mathcal{M}_{mp,nq}.$$

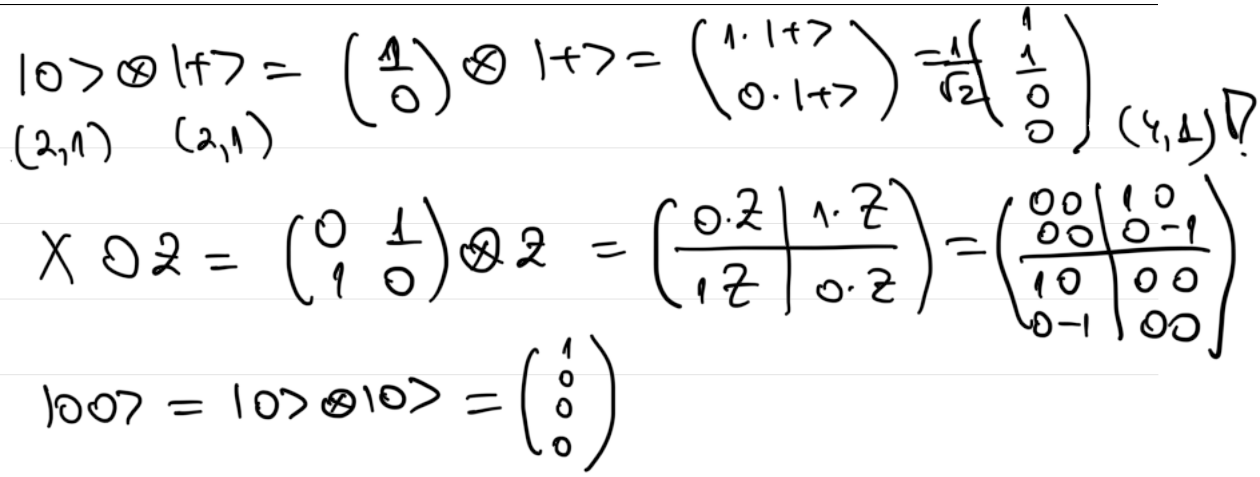
In particular, notice that $A \otimes B$ is defined no matter what the sizes of A and B are (i.e., we do not need to make sure that the sizes of A and B are compatible with each other like we do with standard matrix multiplication). As a result of this, we can also apply the Kronecker product to vectors simply by thinking of them as $1 \times n$ or $m \times 1$ matrices. For this reason, we similarly say that if $v \in \mathbb{F}^m$ and $w \in \mathbb{F}^n$ then the Kronecker product of v and w is

$$v \otimes w := \begin{pmatrix} v_1 w & v_2 w & \dots & v_m w \end{pmatrix} = \begin{pmatrix} v_1 w_1, \dots & v_1 w_1, & v_2 w_1 & \dots & v_2 w_n & \dots & v_m w_1 & v_m w_n \end{pmatrix}$$

Example. *Compute the following tensor product:*

a) $|0\rangle \otimes |+\rangle$

b) $X \otimes Z$ $\in \mathcal{M}_4$.



The above example shows that the Kronecker product is not commutative in general: $A \otimes B$ might not equal $B \otimes A$. However, it does have most of the other "standard" properties that we would expect a matrix product to have, and in particular it interacts with matrix addition and scalar multiplication exactly how we would hope that it does:

Theorem 2.9 — Vector space properties of the Kronecker product

Suppose A, B, and C are matrices with sizes such that the operations below make sense, and let $c \in \mathbb{F}$ be a scalar. Then

a) $(A \otimes B) \otimes C = A \otimes (B \otimes C)$ (associativity)

b) $A \otimes (B + C) = A \otimes B + A \otimes C$ (left distributivity)

c) $(A + B) \otimes C = A \otimes C + B \otimes C$ (right distributivity)

d $(cA) \otimes B = A \otimes (cB) = c(A \otimes B)$.

In particular, associativity of the Kronecker product (i.e., property (a) of the above theorem) tells us that we can unambiguously define Kronecker powers of matrices by taking the Kronecker product of a matrix with itself repeatedly, without having to worry about the exact order in which we perform those products. That is, for any integer $p \geq 1$ we can define

$$A^{\otimes p} := A \otimes A \otimes A \ldots \otimes A$$

Kronecker powers increase in size extremely quickly, since increasing the power by 1 multiplies the number of rows and columns in the result by the number of rows and columns in A, respectively.

Example. *Suppose* $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ *and* $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. *Compute:*

a) $I^{\otimes 2}$,

b) $H^{\otimes 2}$,

$I^{\otimes 2} = I \otimes I = \left(\begin{array}{c|c} 1 \cdot I & 0 \\ \hline 0 & 1 \cdot I \end{array}\right) = I_4$

$H \otimes H$

The Kronecker product also plays well with usual matrix multiplication and other operations like the transpose and inverse. We summarize these additional properties here:

Theorem 2.10 — Algebraic properties of the Kronecker product

Suppose A, B, C, and D are matrices with sizes such that the operations below make sense. Then

a) $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$,

b) $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$, if either of this expression exists

c) $(A \otimes B)^T = A^T \otimes B^T$, and

d) $(A \otimes B)^* = A^* \otimes B^*$, the matrices are complex.

Example. *Compute* $(I \otimes H)(|0\rangle \otimes |0\rangle)$

$(I \otimes H)|0\rangle \otimes |0\rangle = I|0\rangle \otimes H|0\rangle = |0\rangle \otimes |+\rangle$

It is worth noting that Theorems(2.9) and (2.10) still work if we replace all of the matrices by vectors, since we can think of those vectors as $1 \times n$

or $m \times 1$ matrices. Doing this in parts (a) and (d) of the above theorem shows us that if $v, w \in \mathbb{F}^n$ and $x, y \in \mathbb{F}^m$ are (column) vectors, then

$$(v \otimes x) \cdot (w \otimes y) = (v \otimes x)^*(w \otimes y) = (v^* w) \otimes (x^* y) = (v \cdot w) \otimes (x \cdot y).$$

In other words, the dot product of two Kronecker products is just the product of the individual dot products. In particular, this means that $v \otimes x$ is orthogonal to $w \otimes y$ if and only if v is orthogonal to w or x is orthogonal to y (or both).

Properties Preserved by the Kronecker Product

Because the Kronecker product and Kronecker powers can create such large matrices so quickly, it is important to understand how properties of $A \otimes B$ relate to the corresponding properties of A and B themselves. For example, the following theorem shows that we can compute the eigenvalues, determinant, and trace of $A \otimes B$ directly from A and B themselves.

Theorem 2.11 — Eigenvalues, Trace and Determinant if the Kronecker product

Suppose $A \in \mathcal{M}_m$ and $B \in \mathcal{M}_n$.

a) If λ and μ are eigenvalues of A and B, respectively, with corresponding eigenvectors v and w, then $\lambda\mu$ is an eigenvalue of $A \otimes B$ with corresponding eigenvector $v \otimes w$,

b) $tr(A \otimes B) = tr(A)tr(B)$

c) $det(A \otimes B) = (det(A))^n (det(B))^m$

The Kronecker product also preserves several useful families of matrices. For example, it follows straightforwardly from the definition of the Kronecker product that if $A \in \mathcal{M}_m$ and $B \in \mathcal{M}_n$ are both upper triangular, then so is $A \otimes B$. We summarize some observations of this type in the following theorem:

Theorem 2.12 — Matrix properties preserved by the Kronecker product

Suppose $A \in \mathcal{M}_m$ and $B \in \mathcal{M}_n$.

a) If A and B are upper (lower) triangular, so is $A \otimes B$,

b) If A and B are diagonal, so is $A \otimes B$,

c) If A and B are normal, so is $A \otimes B$,

d) If A and B are unitary, so is $A \otimes B$,

e) If A and B are symmetric or Hermitian, so is $A \otimes B$, and

f) If A and B are positive (semi)definite, so is $A \otimes B$.

The Tensor Product

We now introduce an operation, called the tensor product, that combines two vector spaces into a new vector space. This operation can be thought of as a generalization of the Kronecker product that not only lets us multiply together vectors (from $\mathbb{F}^n$) and matrices of different sizes, but also allows us to multiply together vectors from any vector spaces.

Definition 2.22 — Tensor Product

Suppose $\mathcal{V}$ and $\mathcal{W}$ are vector spaces over a field $\mathbb{F}$. Their tensor product is the (unique up to isomorphism) vector space $\mathcal{V} \otimes \mathcal{W}$, also over the field $\mathbb{F}$, with vectors and operations satisfying the following properties:

a) For every pair of vectors $v \in \mathcal{V}$ and $w \in \mathcal{W}$, there is an associated vector (called an elementary tensor) $v \otimes w \in \mathcal{V} \otimes \mathcal{W}$, and every vector in $\mathcal{V} \otimes \mathcal{W}$ can be written as a linear combination of these elementary tensors.

b) Vector addition satisfies

$$v \otimes (w + y) = (v \otimes w) + (v \otimes y)$$

$$(v + x) \otimes w = (v \otimes w) + (x \otimes w), \ \forall v, x \in \mathcal{V}, w, y \in \mathcal{W}$$

c) Scalar multiplication satisfies

$$c(v \otimes w) = (cv) \otimes w = v \otimes (cw) \ \forall c \in \mathbb{F}, v \in \mathcal{V}, w \in \mathcal{W}.$$

d) For every vector space $\mathcal{X}$ over $\mathbb{F}$ and every bilinear transformation $T : \mathcal{V} \times \mathcal{W} \to \mathcal{X}$, there exists a linear transformation

$S : \mathcal{V} \otimes \mathcal{W} \to \mathcal{X}$ such that

$$T(v, w) = S(v \otimes w) \ \forall v \in \mathcal{V}, w \in \mathcal{W}.$$

Theorem 2.13 — Bases of Tensor Products

Suppose $\mathcal{V}$ and $\mathcal{W}$ are vector spaces over the same field with bases B and C, respectively. Then their tensor product $\mathcal{V} \otimes \mathcal{W}$ exists and has the following set as a basis:

$$B \otimes C := \{e \otimes f, e \in B, f \in C\}$$

Since the dimension of a vector space is defined to equal the number of vectors in any of its bases, we immediately get the following corollary that tells us that the dimension of the tensor product of two finite-dimensional vector spaces is just the product of their individual dimensions.

Theorem 2.14 — Dimensionality of Tensor Product

Suppose $\mathcal{V}$ and $\mathcal{W}$ are finite-dimensional vector spaces. Then

$$dim(\mathcal{V} \otimes \mathcal{W}) = dim(\mathcal{V}) dim(\mathcal{W}).$$

Theorem 2.15 — Kronecker Product of Coordinate Vectors

Suppose $\mathcal{V}_1, \mathcal{V}_2, \ldots, \mathcal{V}_p$ are finite vector spaces over the same field with bases $B_1, B_2, \ldots, B_p$, respectively. Then

$$B_1 \otimes B_2 \otimes \ldots \otimes B_p := \{b^{(1)} \otimes b^{(2)} \otimes \ldots \otimes b^{(p)}, b^{(j)} \in B_j, \forall\, 1 \leq j \leq p\}$$

is a basis of $\mathcal{V}_1 \otimes \mathcal{V}_2 \otimes \ldots, \otimes \mathcal{V}_p$ and if we order it lexicographically, then

$$[v_1 \otimes v_2 \otimes \ldots \otimes v_p]_{B_1 \otimes B_2 \otimes \ldots \otimes B_p} = [v_1]_{B_1} \otimes [v_2]_{B_2} \otimes \ldots \otimes [v_p]_{B_p}$$

for all $v_1 \in \mathcal{V}_1, v_2 \in \mathcal{V}_2, \ldots, v_p \in \mathcal{V}_p$.

In the above theorem, when we say that we are ordering the basis $B_1 \otimes$

$B_2 \otimes \ldots \otimes B_p$ lexicographically, we mean that we order it so as to "count" its basis vectors in the most natural way, much like we did for bases of Kronecker product spaces.

For example, if $B_1 = \{v_1, v_2\}$ and $B_2 = \{w_1, w_2, w_3\}$ then we order $B_1 \otimes B_2$ as

$$B_1 \otimes B_2 = \{v_1 \otimes w_1, v_1 \otimes w_2, v_1 \otimes w_3, v_2 \otimes w_1, v_2 \otimes w_2, v_2 \otimes w_3\}$$

> If the space $\mathcal{V}$ associated to some qubits has the basis $\{|0\rangle, |1\rangle\}$, then $\mathcal{V}^{\otimes 2}$ has the basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

$\mathbb{C}^2 \otimes \mathbb{C}^2 \equiv \mathbb{C}^4 \Rightarrow$ $|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$!!

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

Cele mai cunoscute stări entanglement sunt stările Bell $|\phi_+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

$|\phi_-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$

$|\psi_+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$

$|\psi_-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$

Stări separabile $|\varphi\rangle = |a\rangle \otimes |b\rangle$

Dacă nu este separabilă, se numește entangled.

Aratam că starea $|\phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ este entangled, prin reducere la absurd.

Presupunem că $\exists$ vectorii $|a\rangle \otimes |b\rangle$ astfel încât $|\phi_+\rangle = |a\rangle \otimes |b\rangle$ $\Big\}(*)$

Fie $|a\rangle = \begin{pmatrix} x \\ y \end{pmatrix}$; $|b\rangle = \begin{pmatrix} z \\ t \end{pmatrix}$ $\Big\}(*)$

$$|\phi_+\rangle = \begin{pmatrix} x \\ y \end{pmatrix} \otimes \begin{pmatrix} z \\ t \end{pmatrix} = \begin{pmatrix} x|b\rangle \\ y|b\rangle \end{pmatrix} = \begin{pmatrix} xz \\ xt \\ yz \\ yt \end{pmatrix}$$

Deci, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |a\rangle \otimes |b\rangle \Leftrightarrow$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} xz \\ xt \\ yz \\ yt \end{pmatrix} \Rightarrow \begin{cases} xz = \frac{1}{\sqrt{2}} \\ xt = 0 \\ yz = 0 \\ yt = \frac{1}{\sqrt{2}} \end{cases}$$

Caz 1: $x = 0 \Rightarrow$ ec I: $0 = \frac{1}{\sqrt{2}}$ imposibil

Caz 2: $t = 0 \Rightarrow$ ec IV: $0 = \frac{1}{\sqrt{2}}$ imposibil

Deci, $\nexists |a\rangle \otimes |b\rangle$ astfel încât $|a\rangle \otimes |b\rangle = |\phi_+\rangle$

$\Rightarrow$ Deci, $|\phi_+\rangle$ este entangled. ▽