1 Mathematical tools

Hilbert space

A **Hilbert space** is a vector space (of possibly infinite dimension) together with a dot product.

Remark

In this course, we mostly work with $\mathbb{C}^2$. In it, the dot product is defined as:

$$\begin{pmatrix} a \\ b \end{pmatrix} \bullet \begin{pmatrix} c \\ d \end{pmatrix} = a^* c + b^* d$$

where x^* is the complex conjugate of x.

Note that this is so that we can define a norm:

$$\left\| \begin{pmatrix} a \\ b \end{pmatrix} \right\|^2 = \begin{pmatrix} a \\ b \end{pmatrix} \bullet \begin{pmatrix} a \\ b \end{pmatrix} = a^* a + b^* b = |a|^2 + |b|^2 \in \mathbb{R}_+$$

This dot product has almost all the properties of the dot product in $\mathbb{R}^n$, except that it is not commutative:

$$\vec{\boldsymbol{a}} \bullet \vec{\boldsymbol{b}} = \left(\vec{\boldsymbol{b}} \bullet \vec{\boldsymbol{a}}\right)^*$$

We moreover also typically need a transpose operation. Just like in $\mathbb{R}^n$, we want it to be such that:

$$\vec{\boldsymbol{x}} \bullet \vec{\boldsymbol{y}} = \vec{\boldsymbol{x}}^T \vec{\boldsymbol{y}}$$

To work that way, we use the hermitian transpose, written $\vec{\boldsymbol{x}}^\dagger$, which is both a transpose and a complex conjugation:

$$\vec{\boldsymbol{x}} = \begin{pmatrix} a \\ b \end{pmatrix} \implies \vec{\boldsymbol{x}}^\dagger = \left(\vec{\boldsymbol{x}}^T\right)^* = \begin{pmatrix} a^* & b^* \end{pmatrix}$$

Dirac notation

In quantum physics we don't use classical linear algebra notations, but ones that ares typically much more elegant for quantum problems. In it, we write a vector as a ket:

$$|\psi\rangle$$

We can write the text we want inside a ket, here it is a ψ, but we could write $|\text{elephant}\rangle$.

Bra

The hermitian transpose of a ket is written using a bra:

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

That way, the dot product between $|\varphi\rangle$ and $|\psi\rangle$ is given by:

$$\langle\varphi|\psi\rangle$$

As mentioned above, this dot product has many properties of the usual dot product, except that it is not commutative:

$$\langle\varphi|\psi\rangle = \langle\psi|\varphi\rangle^*$$

Basis representation

We may want to represent a ket $|\psi\rangle$ in an orthonormal basis $|A_1\rangle, \ldots, |A_n\rangle$. In other words, we want to find the coefficients $a_1, \ldots, a_n$ such that:

$$|\psi\rangle = \sum_{i=1}^{n} a_i |A_i\rangle$$

To do so, we directly notice that, thanks to the fact that the basis is orthonormal:

$$\langle A_j|\psi\rangle = \sum_i a_i \langle A_j|A_i\rangle = a_i$$

We therefore have the result we wanted:

$$|\psi\rangle = \sum_i \underbrace{\langle A_i|\psi\rangle}_{\in\mathbb{C}} |A_i\rangle = \sum_i |A_i\rangle\langle A_i|\psi\rangle$$

Operators

Operators are simply a generalisation of matrices to a possibly infinite number of dimensions. In this course, we only work with finite-dimension operators, meaning matrices.

An important thing we must be able to do with our operators is diagonalise them, i.e. finding eigenkets (just a fancy name for eigenvectors) and their corresponding eigenvalues. Note that we may write an eigenket of an operator $\hat{A}$ as $|A\rangle$, and its corresponding eigenvalue A. However those three values are different (one is an operator, one is a ket and one is a complex number) and must therefore not be mistaken:

$$\hat{A}|A\rangle = A|A\rangle$$

Operator transpose

We can take the Hermitian transpose of an operator, just like what we do for kets. In this case, it acts on bras instead of kets. This can intuitively be understood with eigenvalues. Let $|A\rangle$ be an eigenket of $\hat{A}$ with eigenvalue a. Then, its corresponding bra is an eigenbra of $\hat{A}^\dagger$:

$$\langle A|\hat{A}^\dagger = \left(\hat{A}|A\rangle\right)^\dagger = \left(a|A\rangle\right)^\dagger = \langle A|a^*$$

However, $|A\rangle$ might not be an eigenket of $\hat{A}^\dagger$.

Operator representation

We might be interested in representing an operator in a basis. To do so, we can notice that:

$$\vec{\boldsymbol{e}}_1^T \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \vec{\boldsymbol{e}}_2 = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = a_{12}$$

Therefore, in a basis $|A_j\rangle$, the operator $\hat{B}$ has components:

$$b_{ij} = \langle A_i|\hat{B}|A_j\rangle$$

This notably means that we can write our operator as:

$$\hat{B} = \sum_{i,j} b_{ij} |A_i\rangle\langle A_j|$$

Again, making a link with 2x2 matrices, this makes sense since:

$$\begin{aligned} & a\begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} + b\begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix} + c\begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \end{aligned}$$

Tensor product

Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be Hilbert spaces of dimensions n and m, respectively. Let $|A_1\rangle, \ldots, |A_n\rangle$ be a basis of the first one, and $|B_1\rangle, \ldots, |B_m\rangle$ be a basis for the second one.

We can construct a new Hilbert space, the **tensor product** of $\mathcal{H}_1$ and $\mathcal{H}_2$, denoted as $\mathcal{H}_1 \otimes \mathcal{H}_2$ such that:

1. It has nm basis kets, written $|A_i\rangle \otimes |B_j\rangle$.
2. $\otimes$ is a linear operation, i.e:
$$\alpha(|\varphi\rangle \otimes |\psi\rangle) = (\alpha|\varphi\rangle) \otimes |\psi\rangle = |\varphi\rangle \otimes (\alpha|\psi\rangle)$$
3. $\otimes$ is distributive over the addition:
$$|\varphi\rangle \otimes (|\psi_1\rangle + |\psi_2\rangle) = |\varphi\rangle \otimes |\psi_1\rangle + |\varphi\rangle \otimes |\psi_2\rangle$$
4. If $\hat{A}$ is an operator that acts on $\mathcal{H}_1$ and $\hat{B}$ acts on $\mathcal{H}_2$, then:
$$\left(\hat{A} \otimes \hat{B}\right)(|\varphi\rangle \otimes |\psi\rangle) = \left(\hat{A}|\varphi\rangle\right) \otimes \left(\hat{B}|\psi\rangle\right)$$
5. The dot product between $|\varphi_1\rangle \otimes |\psi_1\rangle$ and $|\varphi_2\rangle \otimes |\psi_2\rangle$ is given by:
$$(\langle\varphi_1| \otimes \langle\psi_1|)(|\varphi_2\rangle \otimes |\psi_2\rangle) = \langle\varphi_1|\varphi_2\rangle\langle\psi_1|\psi_2\rangle$$
6. The outer product between $|\varphi_1\rangle \otimes |\psi_1\rangle$ and $|\varphi_2\rangle \otimes |\psi_2\rangle$ is given by:
$$(|\varphi_1\rangle \otimes |\psi_1\rangle)(\langle\varphi_2| \otimes \langle\psi_2|) = (|\varphi_1\rangle\langle\varphi_2|) \otimes (|\psi_1\rangle\langle\psi_2|)$$

The three last properties are very close one to another.

Personal remark I'm not sure this definition is completely formal.

Notation 1 When everything is clear, we might write $|\varphi\rangle \otimes |\psi\rangle = |\varphi\psi\rangle$.

Notation 2 Note that, since $|\varphi\rangle$ and $|\psi\rangle$ might be in different Hilbert spaces, the tensor product is definitely not commutative:
$$|\varphi\rangle \otimes |\psi\rangle \neq |\psi\rangle \otimes |\varphi\rangle$$

This may however be a bit cumbersome to always keep those terms in order, especially when have multiple tensor products. Therefore, we might use another notation where, instead of using the order to represent the position in the tensor product, we use numbers outside the kets:
$$|\varphi\rangle_1 \otimes |\psi\rangle_2 = |\psi\rangle_2 \otimes |\varphi\rangle_1$$

This simplifies the notation, but we have to be careful when using it. For instance:
$$(\langle a|_1 \otimes \langle b|_2)(|c\rangle_2 \otimes |d\rangle_1) = \langle a|d\rangle\langle b|c\rangle$$

Property Let $\hat{A}$ and $\hat{B}$ be operators acting in $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Let $|A\rangle$ be an eigenket of $\hat{A}$ with eigenvalue a, and $|B\rangle$ be an eigenket of $\hat{B}$ with eigenvalue b. Then, $|A\rangle \otimes |B\rangle$ is an eigenket of $\hat{A} \otimes \hat{B}$ with eigenvalue ab:
$$\left(\hat{A} \otimes \hat{B}\right)(|A\rangle \otimes |B\rangle) = \left(\hat{A}|A\rangle\right) \otimes \left(\hat{B}|B\rangle\right) = ab|A\rangle \otimes |B\rangle$$

Basis representation

Let $|\varphi\rangle \in \mathcal{H}_1$ and $|\psi\rangle \in \mathcal{H}_2$. Let's suppose that we can represent them in the bases of $\mathcal{H}_1$ and $\mathcal{H}_2$:

$$|\varphi\rangle = \sum_i \varphi_i |A_i\rangle, \quad |\psi\rangle = \sum_j \psi_j |B_j\rangle$$

Then, we can use all our properties to represent $|\varphi\rangle \otimes |\psi\rangle$ in the basis $|A_iB_j\rangle = |A_i\rangle \otimes |B_j\rangle$:

$$|\varphi\rangle \otimes |\psi\rangle = \left(\sum_i \varphi_i |A_i\rangle\right) \otimes \left(\sum_j \psi_j |B_j\rangle\right) = \sum_{i,j} \varphi_i \psi_j |A_i B_j\rangle$$

This directly gives us that the coefficients are $\varphi_i\psi_j$. We can translate this in array form. If $|\varphi\rangle = \begin{pmatrix} a & b \end{pmatrix}^T$ and $|\psi\rangle = \begin{pmatrix} c & d \end{pmatrix}^T$, we have, ordering the basis as $(|A_0B_0\rangle, |A_0B_1\rangle, |A_1B_0\rangle, |A_1B_1\rangle)$:

$$|\varphi\rangle \otimes |\psi\rangle = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} = \begin{pmatrix} a|\psi\rangle \\ b|\psi\rangle \end{pmatrix}$$

It is possible to generalise this to general operators, and get that, in array form:

$$\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \otimes \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} = \begin{pmatrix} a_{00}b_{00} & a_{00}b_{01} & a_{01}b_{00} & a_{01}b_{01} \\ a_{00}b_{10} & a_{00}b_{11} & a_{01}b_{10} & a_{01}b_{11} \\ a_{10}b_{00} & a_{10}b_{01} & a_{11}b_{00} & a_{11}b_{01} \\ a_{10}b_{10} & a_{10}b_{11} & a_{11}b_{10} & a_{11}b_{11} \end{pmatrix}$$
$$= \begin{pmatrix} a_{00}B & a_{01}B \\ a_{10}B & a_{11}B \end{pmatrix}$$

Unitary operator An operator $\hat{A}$ is said to be **unitary** if:

$$\hat{A}^\dagger \hat{A} = \hat{I}$$

where $\hat{I}$ is the identity operator.

Property 1

Note that we have the following equivalence:

$$\hat{A}^\dagger \hat{A} = \hat{I} \iff \hat{A}\hat{A}^\dagger = \hat{I}$$

One can therefore check any of those two to prove that an operator is unitary.

Property 2

Unitary operators preserve the norm:

$$\left\| \hat{A}|\psi\rangle \right\| = \||\psi\rangle\|$$

This can be shown directly, using the squared norm:

$$\left\| \hat{A}|\psi\rangle \right\|^2 = \langle\psi|A^\dagger A|\psi\rangle = \langle\psi|\psi\rangle = \||\psi\rangle\|^2$$

Hermitian operator An operator $\hat{A}$ is said to be **hermitian** if:

$$\hat{A}^\dagger = \hat{A}$$

Spectral theorem Let $\hat{A}$ be an Hermitian operator. Then, it can be diagonalised into an orthonormal eigenbasis with real eigenvalues.

In other words, we can find eigenkets $|A_1\rangle, \dots, |A_n\rangle$ such that their corresponding eigenvalues are real, and:

$$\langle A_i | A_j \rangle = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$$

Implication This means that we can write any Hermitian operator as:

$$\hat{A} = \sum_i a_i |A_i\rangle\langle A_i|$$

where $|A_i\rangle$ are eigenkets of $\hat{A}$ and a_i are the corresponding eigenvalues.

Indeed, we know that the coefficient a_{ij} of $\hat{A}$ is given by:

$$a_{ij} = \langle A_i | \hat{A} | A_j \rangle = a_j \langle A_i | A_j \rangle = \begin{cases} a_j, & \text{if } i = j \\ 0, & \text{otherwise} \end{cases}$$

This justifies why we use the term "diagonalise": in this basis, $\hat{A}$ is diagonal.

Semi-positive definite operator An operator $\hat{A}$ is **semi-postive definite** if all its eigenvalues are nonnegative. Equivalently:

$$\langle \psi | A | \psi \rangle \geq 0, \quad \forall |\psi\rangle$$

Operator exponential Let $\hat{A}$ be an operator. Its exponential is defined as:

$$\exp\left(\hat{A}\right) = \sum_{n=0}^{\infty} \frac{\hat{A}^n}{n!}$$

Property 1 We have that:

$$\frac{d}{dt} \exp\left(\hat{A}t\right) = \hat{A} \exp\left(\hat{A}t\right)$$

This is the property that justifies this definition. It notably means that the general solution to $\hat{A}|\psi(t)\rangle = \frac{d}{dt}|\psi(t)\rangle$ is:

$$|\psi(t)\rangle = \exp(At)|\psi(0)\rangle$$

Property 2 Let $|A\rangle$ be an eigenket of $\hat{A}$ of eigenvalue a. Then:

$$\exp\left(\hat{A}\right)|A\rangle = \exp(a)|A\rangle$$

In other words, the eigenvectors of $\hat{A}$ and $\exp\left(\hat{A}\right)$ are the same, with eigenvalues a and $\exp(a)$ respectively.

Indeed, this can be shown directly:

$$\exp\left(\hat{A}\right)|A\rangle = \sum_{n=0}^{\infty} \frac{\hat{A}^n |A\rangle}{n!} = \sum_{n=0}^{\infty} \frac{a^n |A\rangle}{n!} = \exp(a)|A\rangle$$

Property 3 If two operators commute, meaning $\hat{A}\hat{B} = \hat{B}\hat{A}$, then:

$$\exp\left(\hat{A}\right) \exp\left(\hat{B}\right) = \exp\left(\hat{A} + \hat{B}\right)$$

Note that this is not true in general if the operators do not commute.

Operator logarithm Let $\hat{A}$ be a semi-positive definite hermitian operator. We know we can find eigenvectors $|A_j\rangle$ with non-negative real eigenvalues $a_j \geq 0$, yielding that it can be written as:

$$\hat{A} = \sum_j a_j |A_j\rangle\langle A_j|$$

Its logarithm is defined as:

$$\ln\left(\hat{A}\right) = \sum_j \ln(a_j)|A_j\rangle\langle A_j|$$

> *Remark* By definition, this yields that:
>
> $$\ln\left(\hat{A}\right)|A_j\rangle = \ln(a_j)|A_j\rangle$$
>
> In other words, the eigenvectors of $\hat{A}$ and $\ln\left(\hat{A}\right)$ are the same, with eigenvalues a_i and $\ln(a_i)$ respectively.

Trace The **trace** of an operator $\hat{A}$ is defined as the sum of its diagonal elements:

$$\mathrm{Tr}\left(\hat{A}\right) = \sum_{i=1}^{n} \langle B_i|\hat{A}|B_i\rangle$$

where $\{|B_i\rangle\}$ is an arbitrary basis, the choice of which does not change the result.

> *Property 1* If $\hat{A}$ can be diagonalised, we can take $\{|B_i\rangle\}$ to be a basis of eigenvectors of $\hat{A}$, yielding that, in this case, $\mathrm{Tr}\left(\hat{A}\right)$ is the sum of eigenvalues of $\hat{A}$.

> *Property 2* The trace is cyclic. This means that, if the multiplications make sense:
>
> $$\mathrm{Tr}\left(\hat{A}\hat{B}\right) = \mathrm{Tr}\left(\hat{B}\hat{A}\right)$$
>
> This for instance yields that:
>
> $$\mathrm{Tr}\left(\hat{A}\hat{B}\hat{C}\right) = \mathrm{Tr}\left(\hat{C}\hat{A}\hat{B}\right)$$
>
> However, in general:
>
> $$\mathrm{Tr}\left(\hat{A}\hat{B}\hat{C}\right) \neq \mathrm{Tr}\left(\hat{A}\hat{C}\hat{B}\right)$$

Partial trace Let $\hat{A}$ be an operator acting on a Hilbert space $\mathcal{H}_{S\cup E} = \mathcal{H}_S \otimes \mathcal{H}_E$, and let $|A_j\rangle \otimes |B_i\rangle$ be a basis of this Hilbert space for $j \in \{1, \ldots, J\}$ and $i \in \{1, \ldots, I\}$. The (k, ℓ) component of the **partial trace** of $\hat{A}$ with respect to $\mathcal{H}_S$ is:

$$\left(\mathrm{Tr}_{\mathcal{H}_S}\left(\hat{A}\right)\right)_{k,\ell} = \sum_{j=1}^{J} \hat{A}_{(j,k),(j,\ell)} = \sum_{j=1}^{J} \langle A_j B_k|\hat{A}|A_j B_\ell\rangle$$

This is a $I \times I$ matrix.

> *Property 1* Just like the regular trace, the partial trace is additive:
>
> $$\mathrm{Tr}_{\mathcal{H}_S}\left(\hat{A} + \hat{B}\right) = \mathrm{Tr}_{\mathcal{H}_S}\left(\hat{A}\right) + \mathrm{Tr}_{\mathcal{H}_S}\left(\hat{B}\right)$$

> *Property 2* If our operator can be written as $\hat{A} = \hat{S} \otimes \hat{E}$, then:
>
> $$\mathrm{Tr}_{\mathcal{H}_S}\left(\hat{A}\right) = \mathrm{Tr}\left(\hat{S}\right)\hat{E}$$

Example Let us consider an arbitrary operator:

$$\hat{A} = \sum_{i,j,i',j'} a_{i,j,i',j'} |A_i B_j\rangle\langle A_{i'} B_{j'}|$$

We notice that we can always write it as:

$$\hat{A} = \sum_{i,i'} |A_i\rangle\langle A_{i'}| \otimes \left(\sum_{j,j'} a_{ij,i',j'} |B_j\rangle\langle B_{j'}| \right)$$

This allows us to compute its partial trace, thanks to its properties:

$$\mathrm{Tr}_{\mathcal{H}_S}\left(\hat{A}\right) = \sum_{i,i'} \mathrm{Tr}(|A_i\rangle\langle A_{i'}|) \sum_{j,j'} a_{ij,i',j'} |B_j\rangle\langle B_{j'}|$$

Now, by the cylicity of the trace:

$$\mathrm{Tr}(|A_i\rangle\langle A_{i'}|) = \mathrm{Tr}(\langle A_{i'}|A_i\rangle) = \langle A_{i'}|A_i\rangle = \begin{cases} 1, & \text{if } i = i' \\ 0, & \text{if } i \neq i' \end{cases}$$

This finally yields:

$$\mathrm{Tr}_{\mathcal{H}_S}\left(\hat{A}\right) = \sum_{i,j,j'} a_{i,j,i,j'} |B_j\rangle\langle B_{j'}|$$

which is indeed $I \times I$.

Intuitively, this means that, to compute the coefficient at j, j' in basis $|B_j\rangle$, we take the trace of the submatrices where j and j' are constant (i.e., we compute the sum of the diagonal elements of those submatrices). For instance, for $\mathbb{C}^2 \otimes \mathbb{C}^2$, ordering the basis as $|A_0 B_0\rangle, |A_1 B_0\rangle, |A_0 B_1\rangle, |A_1 B_1\rangle$ (this is not the classical basis ordering, but it allows a better visualisation):

$$\begin{aligned} \mathrm{Tr}_{\mathcal{H}_S} \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{pmatrix} &= \begin{pmatrix} \mathrm{Tr}\begin{pmatrix} a & b \\ e & f \end{pmatrix} & \mathrm{Tr}\begin{pmatrix} c & d \\ g & h \end{pmatrix} \\ \mathrm{Tr}\begin{pmatrix} i & j \\ m & n \end{pmatrix} & \mathrm{Tr}\begin{pmatrix} k & l \\ o & p \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} a + f & c + h \\ i + n & k + p \end{pmatrix} \end{aligned}$$

2 Axioms

Superposition The state of a quantum system is a vector $|\psi\rangle$ in a Hilbert space of field $\mathbb{C}$. This vector is normalised:

$$\langle\psi|\psi\rangle = 1$$

Each possible state that could be obtained after a measurement yields a different orthonormal basis.

Example For instance, if a photon can either go through a mirror or not, the dimension of the corresponding Hilbert space is 2, and any state can be represented as:

$$a|\text{went through}\rangle + b|\text{bounced}\rangle$$

However measuring the position of a particle yields a Hilbert space of infinite dimensions since there are infinitely many possibilities after every measurement.

Composition of quantum systems

The composition of two quantum systems which are described by Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively, is described by the tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Born rule

There is a one-to-one correspondance between hermitian operator and observables (something that we can measure). In other words, the result of any physical measurement can be represented by a hermitian operator, and any hermitian operator can be measured.

Let $\hat{A}$ be the hermitian operator linked to a measurement. By the spectral theorem, we know we can find orthonormal eigenkets $|A_1\rangle, \ldots, |A_n\rangle$ with real eigenvalues $a_1, \ldots, a_n$. When we use it to measure a state $|\psi\rangle$, we measure one of the eigenvalues a_i and the state collapses to $|A_i\rangle$, the i being chosen with probability:

$$|\langle A_i|\psi\rangle|^2$$

Note that the fact that the eigenvalues are real is very important, since we can never measure a complex value in physics.

> *Intuition*
>
> Representing our state in the basis formed by the eigenkets of $\hat{A}$ helps us understand what is happening:
>
> $$|\psi\rangle = \psi_1|A_1\rangle + \ldots + \psi_n|\psi_n\rangle$$
>
> Since the eigenkets are orthonormal, we have:
>
> $$\langle A_i|\psi\rangle = \psi_i$$
>
> which it the i^{th} composant of the vector $|\psi\rangle$ in the basis of the eigenkets of $\hat{A}$.
>
> We can moreover verify that the probabilities sum to 1:
>
> $$\sum_{i=1}^{n} \mathbb{P}(\text{collapses to } i) = \sum_{i=1}^{n} |\langle A_i|\psi\rangle|^2 = \sum_{i=1}^{n} |\psi_i|^2 = \langle\psi|\psi\rangle = \||\psi\rangle\|^2 = 1$$

> *Remark*
>
> In many cases, it is worth noticing that:
>
> $$|\langle\varphi|\psi\rangle|^2 = \langle\varphi|\psi\rangle^* \langle\varphi|\psi\rangle = \langle\psi|\varphi\rangle\langle\varphi|\psi\rangle$$
>
> More generally, computing norms using the complex conjugates often helps to compute those values much more easily. For instance:
>
> $$\left|1 + e^{i\theta}\right| = \left(1 + e^{-i\theta}\right)\left(1 + e^{i\theta}\right) = 1 + e^{i\theta - i\theta} + e^{i\theta} + e^{-i\theta} = 2 + 2\cos(\theta)$$

Partial measurement

In a quantum system described by a Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$, we can do a measurement on a state $|\psi\rangle$ using an observable $\hat{A}$ on one of the particules (let's say the one of $\mathcal{H}_1$), while leaving the other untouched. The particule collapses to some eigenket $|A_i\rangle$, and the whole states becomes proportional to:

$$c|\psi'\rangle = \Big(|A_i\rangle\langle A_i| \otimes \hat{I}\Big)|\psi\rangle = \hat{P}|\psi\rangle$$

The term $\hat{P}$ is named a projector, and we can verify that it is such that $\hat{P}^\dagger = \hat{P}$ and $\hat{P}^2 = \hat{P}$. The probability that this i is chosen is given by:

$$|c|^2 = \left\|\hat{P}|\psi\rangle\right\|^2 = \langle\psi|\hat{P}|\psi\rangle$$

> *Remark*
>
> This a generalisation of the born rule. Indeed, we can always write our particle using the orthonormal basis given by the eigenkets of

$\hat{A}$ for $\mathcal{H}_1$, and another orthonormal basis for $\mathcal{H}_2$:

$$|\psi\rangle = \sum_{i,j} \psi_{i,j} |A_i B_j\rangle$$

We can then write this state as:

$$|\psi\rangle = \sum_i |A_i\rangle \otimes \left(\sum_j \psi_{i,j} |B_j\rangle \right)$$

Therefore, it makes sense that, when we measure and the state of the first particle collapses to $|A_i\rangle$, then the whole state simply collapses to something proportional to:

$$c|\psi'\rangle = |A_i\rangle \otimes \left(\sum_j \psi_{i,j} |B_j\rangle \right) = \sum_j \psi_{i,j} |A_i B_j\rangle$$

Then, the probability that it happens is given by:

$$|c|^2 = \left\|c|\psi'\rangle\right\|^2 = \left\| \sum_j \psi_{i,j} |A_i B_j\rangle \right\|^2 = \sum_j |\psi_{i,j}|^2$$

which is indeed a generalisation of the Born rule.

Unitary time evolution

Let $|\psi(t)\rangle$ be a quantum state at time t living in an isolated system. Its time evolution is given by an operator $\hat{U}(t_1, t_0)$, which is such that:

$$|\psi(t_1)\rangle = \hat{U}(t_1, t_0) |\psi(t_0)\rangle$$

This operator must have the following properties:

1. $\hat{U}$ is unitary.
2. $\hat{U}(t_2, t_1)\hat{U}(t_1, t_0) = \hat{U}(t_2, t_0)$

It is also possible to be given a time-evolution operator, which does not depend on time. This gives a way to describe a state after enough time has passed (supposing $\hat{U}(t, t_0) = \hat{I}$ for any big enough t). In this case, all we need to verify is that this operator is unitary.

Intuition The first property is necessary for $\psi(t)$ to always be normalised, when we start with a normalised state $\psi(t_0)$: recall that unitary operator preserve the norm.

The second property means that leaving the system evolve from a time t_0 to t_1 and then from t_1 to t_2 is equivalent to letting it evolve from t_0 to t_2.

Notation We typically write:

$$\hat{U}(t, 0) = \hat{U}(t)$$

Remark It is possible to show that those properties require $|\psi(t)\rangle = \hat{U}|\psi(0)\rangle$ respects the following differential equation, named **Schrödinger's equation**:

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = \hat{H} |\psi(t)\rangle$$

where $\hat{H}$ is an Hermitian operator, i.e. an observable; and $\hbar$ is a physical constant that notably allows $\hat{H}$ to have the unit of energy.

This $\hat{H}$ is named the **Hamiltonian**. It is very important: it is what describes the time evolution. By doing a deeper analysis, we can make a link with the classical case to consider this as the energy of the system. In other words, when we measure this observable, we will get a real value (as for any observable), which is the energy of the system.

Note that if $\hat{H}$ does not depend on time, the general solution is then just:

$$\hat{U}(t) = \exp\left(-\frac{i}{\hbar}\hat{H}t\right)$$

This can be solved by finding the eigenkets of $\hat{H}$, $|E_1\rangle, \ldots, |E_n\rangle$ with eigenvalues $E_1, \ldots, E_n$ since:

$$\begin{aligned} |\psi(t)\rangle &= \exp\left(-\frac{i}{\hbar}\hat{H}t\right)|\psi(0)\rangle \\ &= \exp\left(-\frac{i}{\hbar}\hat{H}t\right)(\psi_1|E_1\rangle + \ldots + \psi_n|E_n\rangle) \\ &= \psi_1 \exp\left(-\frac{i}{\hbar}E_1 t\right)|E_1\rangle + \ldots + \psi_n \exp\left(-\frac{i}{\hbar}E_n t\right)|E_n\rangle \end{aligned}$$

where we used the fact that $\exp\left(\hat{H}\right)|E_1\rangle = \exp(E_1)|E_1\rangle$, as explained when describing exponential of matrices. This is the representation of $|\psi(t)\rangle$ in the eigenbasis $|E_1\rangle, \ldots, |E_n\rangle$.

3 Quantum physics

Global phase We notice that none of the axioms allow us to get the global phase of some state: there is no way to let a state evolve in time in some system and to then do a measurement that would allow us to measure its global phase. This means that, for any $\gamma \in \mathbb{R}$, the two following states are physically equivalent:

$$e^{i\gamma}|\psi\rangle \equiv |\psi\rangle$$

Remark Note however that we cannot say the same of local phase. The two following states are physically different:

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \not\equiv \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Expected values The expected value got when measuring a state $|\psi\rangle$ with an observable $\hat{A}$, written $\left\langle \hat{A} \right\rangle_\psi$, is given by:

$$\left\langle \hat{A} \right\rangle_\psi = \langle\psi|\hat{A}|\psi\rangle$$

Intuition Recall that, when doing a measure, a state changes. Therefore, this value can be measure experimentally by preparing a particle in state $|\psi\rangle$, measuring it using $\hat{A}$, preparing another particle in this state $|\psi\rangle$ and so on.

Proof By the Born rule, when we measure a state using an operator $\hat{A}$, the state collapses to some eigenket $|A_i\rangle$ with probability $|\langle A_i|\psi\rangle|^2$, and the measure gets a_i. Therefore, the expected value is given by:

$$\begin{aligned}\left\langle \hat{A} \right\rangle_\psi &= \sum_i a_i \mathbb{P}(\text{collapsed to } i)\\ &= \sum_i a_i |\langle A_i|\psi\rangle|^2\\ &= \sum_i a_i \langle \psi|A_i\rangle\langle A_i|\psi\rangle\\ &= \langle\psi|\left(\sum_i a_i |A_i\rangle\langle A_i|\right)|\psi\rangle\end{aligned}$$

We recognise the sum to be the diagonal representation of $\hat{A}$ in its eigenbasis, giving us our result:

$$\left\langle \hat{A} \right\rangle_\psi = \langle\psi|\hat{A}|\psi\rangle$$

□

Q-bit

To represent q-bits, we need quantum states that live in $\mathcal{H} = \mathbb{C}^2$, i.e. which have two possibilities.

The physical way to represent this is to consider the spin of electrons (some kind of intrinsic properties that is analogous to the electron spinning on itself). Since electrons are spin-$\frac{1}{2}$ particles, they only have two possibility when we measure their spin in some $\hat{z}$ direction: up $|0\rangle$ or down $|1\rangle$. This is named the computation basis. When we measure the up particle we register a 1, and when we measure a down, we register a -1, giving us that our observable is:

$$\hat{\sigma}_z = 1|0\rangle\langle 0| - 1|1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Now, it is possible to measure the spin in other directions, $\hat{x}$ and $\hat{y}$. Doing so, we can make physical experiments to see that measuring in one direction, then in an orthogonal one, and then back in the first one, the first and third measure will not necessarily yield the same result. This basically means that the second measure destroyed the value we measured. It is possible to show that the observable linked to those measurement directions can be chosen to be:

$$\hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \hat{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

The eigenkets of $\hat{\sigma}_x$ are quite important. They are given by:

$$\hat{H}|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad \hat{H}|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

where $\hat{H}$ is an important matrix, named the **Hadamard matrix**:

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

Pauli matrices

The matrices $\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z$ are so important they are given a name, they are the **Pauli matrices**. They are sometimes written:

$$\hat{X} = \hat{\sigma}_x, \quad \hat{Y} = \hat{\sigma}_y, \quad \hat{Z} = \hat{\sigma}_z$$

Those matrices all have the following properties:

$$\hat{\sigma}_z = \hat{\sigma}_z^\dagger, \quad \hat{\sigma}_z^2 = \hat{I}$$

Moreover, by construction, their eigenvalues are -1 and 1 (the values that are measured when using them as observables).

Finally, we sometimes need to consider $a_x\hat{\sigma}_x + a_y\hat{\sigma}_y + a_z\hat{\sigma}_z$. To do so, we use a pseudo-vector:

$$\vec{\boldsymbol{\sigma}} = \begin{pmatrix} \hat{\sigma}_x \\ \hat{\sigma}_y \\ \hat{\sigma}_z \end{pmatrix}$$

Then, leaving $\vec{\boldsymbol{a}} = \begin{pmatrix} a_x & a_y & a_z \end{pmatrix}^T$, we simply have:

$$\vec{\boldsymbol{a}} \bullet \vec{\boldsymbol{\sigma}} = a_x\hat{\sigma}_x + a_y\hat{\sigma}_y + a_z\hat{\sigma}_z$$

This must mostly be understood as some notation shortcut, more than a meaningful definition.

Light polarisation

It is also possible to define the q-bits using light polarisation. If the light is horizontally polarised we note $|0\rangle$, and if it is vertically polarised we note $|1\rangle$. This can be measured using a horizontal polariser filter, followed by photodector. If the detector clicks, the photon was not absorbed and thus collapsed to its horizontal polarisation state. If the detector does not click, the photon was absorbed by the filter, and thus collapsed to its vertical state. Then, $\hat{\sigma}_x$ is equivalent to a polariser filter which is at 45° and $\hat{\sigma}_y$ is equivalent to measuring light circular polarisation.

This is a completely equivalent definition, but it allows to make sense of the following eigenbasis, which is appears when setting the polariser at angle α:

$$|\alpha\rangle = \cos(\alpha)|0\rangle + \sin(\alpha)|1\rangle, \quad |\alpha_\perp\rangle = -\sin(\alpha)|0\rangle + \cos(\alpha)|1\rangle$$

Notation

As a reference to spins, it is possible to write:

$$|0\rangle = |\uparrow\rangle, \quad |1\rangle = |\downarrow\rangle$$

Euler's identity for operators

Let $\hat{A}$ be an operator such that $\hat{A}^2 = 1$. Then:

$$\exp\left(i\theta\hat{A}\right) = \cos(\theta)\hat{I} + i\sin(\theta)\hat{A}$$

Remark

This is in particular valid for:

$$\hat{A} = \vec{\boldsymbol{n}} \bullet \vec{\boldsymbol{\sigma}}$$

where $\vec{\boldsymbol{n}}$ is a unit vector, i.e. $\vec{\boldsymbol{n}} \bullet \vec{\boldsymbol{n}} = 1$.

This can be useful when solving Schrödinger's equation.

Proof

We notice that, for any n:

$$\hat{A}^{2n} = \left(\hat{A}^2\right)^n = \hat{I}^n = \hat{I}$$

Therefore, using the definition of the operator exponential, and splitting the sum on the even and odd terms, we get:

$$\begin{aligned}\exp\left(i\theta\hat{A}\right) &= \sum_{n=0}^{\infty}\frac{\left(i\theta\hat{A}\right)^n}{n!}\\ &= \sum_{n=0}^{\infty}\frac{\left(i\theta\hat{A}\right)^{2n}}{(2n)!}+\sum_{n=0}^{\infty}\frac{\left(i\theta\hat{A}\right)^{2n+1}}{(2n+1)!}\\ &= \sum_{n=0}^{\infty}\frac{\left(i^2\right)^n\theta^{2n}\left(\hat{A}^2\right)^n}{(2n)!}+i\hat{A}\sum_{n=0}^{\infty}\frac{\left(i^2\right)^n\theta^{2n+1}\left(\hat{A}^2\right)^n}{(2n+1)!}\\ &= \hat{I}\sum_{n=0}^{\infty}\frac{(-1)^n\theta^{2n}}{(2n)!}+i\hat{A}\sum_{n=0}^{\infty}\frac{(-1)^n\theta^{2n+1}}{(2n+1)!}\end{aligned}$$

which gives our result, recognising the Taylor expansions of $\cos(\theta)$ and $\sin(\theta)$.

□

Entangled state Let $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ be some state, such that we can find $|\varphi_1\rangle \in \mathcal{H}_1$ and $|\varphi_2\rangle \in \mathcal{H}_2$ where:

$$|\psi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$$

Then, this sate is named a **product state**. If there does not exist such $|\varphi_1\rangle, |\varphi_2\rangle$, it is named an **entangled state**.

Characterisation We want to characterise when a state $|\psi\rangle$ that lives in a Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2$ is entangled. $|\psi\rangle$ can always be written as:

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

Then, $|\varphi_1\rangle \otimes |\varphi_2\rangle$ can always be written as:

$$\begin{aligned}|\varphi_1\rangle \otimes |\varphi_2\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)\\ &= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle\end{aligned}$$

For the two equations to be equal, all components must be equal. We can represent this equation using matrices:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \alpha\gamma & \alpha\delta \\ \beta\gamma & \beta\delta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}\begin{pmatrix} \gamma & \delta \end{pmatrix}$$

However, the matrix on the right has rank 1. For the state to be a product state, we also need the matrix on the left to be rank 1. We can show that this implies that a state living in $\mathbb{C}^2 \otimes \mathbb{C}^2$ is a product state if and only if:

$$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = 0 \iff ad - bc = 0$$

Bell states The following states are examples of “very-entangled” states; that are, in some form the most entangled states in $\mathbb{C}^2 \otimes \mathbb{C}^2$ can possibly be. They are named **Bell sates** or **EPR pairs**:

$$\begin{aligned}|B_{00}\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad |B_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}},\\ |B_{10}\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \quad |B_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.\end{aligned}$$

We can notice that they are orthonormal. Thus, we can make an observable which eigenkets are the bell states.

Property It does not matter the basis we choose to represent those states:

$$|B_{00}\rangle = \frac{|\alpha\alpha\rangle + |\alpha_\perp\alpha_\perp\rangle}{\sqrt{2}}$$

and similarly for the other states.

This can be shown directly by computing the elements in the computation basis:

$$\langle 00|B_{00}\rangle = \frac{\cos(\alpha)^2 + \sin(\alpha)^2}{\sqrt{2}} = \frac{1}{\sqrt{2}}$$

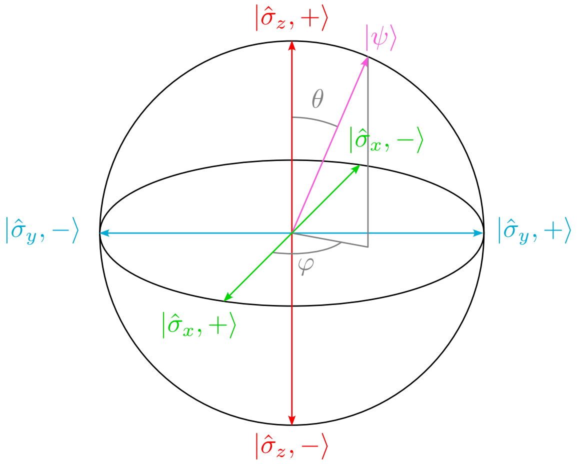
$$\langle 01|B_{00}\rangle = \frac{\cos(\alpha)\sin(\alpha) - \sin(\alpha)\cos(\alpha)}{\sqrt{2}} = 0$$

and similarly for the other terms, indeed yielding that $|B_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.

Bloch sphere Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathbb{C}^2$ be an arbitrary q-bit. Then, there exists unique $\theta \in [0, \pi]$ and $\varphi \in [0, 2\pi[$ such that $|\psi\rangle$ is physically equivalent to:

$$|\psi\rangle \equiv \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\varphi}|1\rangle$$

Interpretation This means that we can always represent a q-bit on a sphere, using θ and φ as spherical coordinates.


$|\hat{\sigma}_z, +\rangle$
$|\psi\rangle$
θ
$|\hat{\sigma}_x, -\rangle$
$|\hat{\sigma}_y, -\rangle$
$|\hat{\sigma}_y, +\rangle$
φ
$|\hat{\sigma}_x, +\rangle$
$|\hat{\sigma}_z, -\rangle$

The north pole is the eigenket of $\hat{\sigma}_z$ with positive eigenvalue $|0\rangle$ (written as $|\hat{\sigma}_z, +\rangle$ on the diagram) and the south pole is the eigenket of $\hat{\sigma}_z$ with negative eigenvalue $|1\rangle$ (written as $|\hat{\sigma}_z, -\rangle$). On the equator, there are the eigenkets of $\hat{\sigma}_x$ and $\hat{\sigma}_y$.

Thus, in some form, θ tells us how close we are to an eigenket of $\hat{\sigma}_z$, and φ how close to an eigenket of $\hat{\sigma}_x$ and $\hat{\sigma}_y$.

We finally notice that the ket that is orthonormal to some ket $|\psi\rangle$ is simply the one that goes to the opposite point on the sphere (the north pole for the south pole, for instance).

Proof Let us represent $\alpha, \beta \in \mathbb{C}$ in their polar coordinates:

$$|\psi\rangle = ae^{i\delta}|0\rangle + be^{i\gamma}|1\rangle$$

for $a, b \in \mathbb{R}_+$ and $\delta, \gamma \in [0, 2\pi[$.

Since the global phase does not matter, this state is physically equivalent to:

$$|\psi\rangle = e^{i\delta}\Big(a|0\rangle + be^{i(\gamma-\delta)}|1\rangle\Big) \equiv a|0\rangle + be^{i(\gamma-\delta)}|1\rangle$$

Since this is a quantum state, we moreover have the normalisation constraint that:

$$|\alpha|^2 + |\beta|^2 = 1 \iff a^2 + b^2 = 1$$

Together with the fact that $a > 0$ and $b > 0$, this constraint yields by the parametrisation of the circle that we can always find an angle $\frac{\theta}{2} \in \big[0, \frac{\pi}{2}\big[$ such that:

$$a = \cos\left(\frac{\theta}{2}\right), \quad b = \sin\left(\frac{\theta}{2}\right)$$

This gives our result by leaving $\varphi = (\gamma - \delta) \bmod 2\pi$.

No cloning theorem

Let $|\varphi_1\rangle \neq |\varphi_2\rangle$ be two states that are not orthonormal:

$$\langle\varphi_1|\varphi_2\rangle = 0$$

Then, there exists no $\hat{U}$ and $|o\rangle$ for which:

$$\hat{U}|\varphi_1\rangle \otimes |o\rangle = |\varphi_1\rangle \otimes |\varphi_1\rangle, \quad \hat{U}|\varphi_2\rangle \otimes |o\rangle = |\varphi_2\rangle \otimes |\varphi_2\rangle$$

Intuition

This theorem is very restrictive. It notably means that we cannot make a "cloning machine" which would allow to copy an arbitrary state $|\varphi\rangle$ onto a blank state $|o\rangle$, without destroying the first state. In other words, there does not exist a $\hat{U}$ and $|o\rangle$ such that:

$$\hat{U}|\varphi\rangle \otimes |o\rangle = |\varphi\rangle \otimes |\varphi\rangle, \quad \forall|\varphi\rangle$$

Proof

We suppose towards contradiction that this $\hat{U}$ and $|o\rangle$ exists, giving us:

$$\hat{U}|\varphi_1\rangle \otimes |o\rangle = |\varphi_1\rangle \otimes |\varphi_1\rangle, \quad \hat{U}|\varphi_2\rangle \otimes |o\rangle = |\varphi_2\rangle \otimes |\varphi_2\rangle$$

Multiplying the Hermitian transpose of the first equation with the second one, we get:

$$\langle\varphi_1| \otimes \langle o|\hat{U}^\dagger\hat{U}|\varphi_2\rangle \otimes |o\rangle = (\langle\varphi_1| \otimes \langle\varphi_1|)(|\varphi_2\rangle \otimes |\varphi_2\rangle)$$

Now, we know that $\hat{U}^\dagger\hat{U} = \hat{I}$ by the time evolution principle, giving us that:

$$\langle\varphi_1|\varphi_2\rangle\langle o|o\rangle = \langle\varphi_1|\varphi_2\rangle\langle\varphi_1|\varphi_2\rangle \iff \langle\varphi_1|\varphi_2\rangle(1 - \langle\varphi_1|\varphi_2\rangle) = 0$$

This either means that $\langle\varphi_1|\varphi_2\rangle = 0$, which yields that they are orthonormal, or $\langle\varphi_1|\varphi_2\rangle = 1$, which yields that $|\varphi_1\rangle = |\varphi_2\rangle$. Both cases are not possible by hypothesis, which gives us our contradiction.

□

Bell inequalities

A source sends an EPR pair split between Alice and Bob (each have one q-bit). Alice has two possible measurement bases, $\{|\alpha\rangle, |\alpha_\perp\rangle\}$ at angle α, and one at angle α'. We model her part of the experiment using two random variables: A and A'. $A \in \{-1, 1\}$ is the value she would get if she used the basis α, and similarly for

A'. Completely analogously, Bob has two measurement bases β and β', which measurement results are B and B'.

It is possible to measure experimentally the following value:

$$x = \mathbb{E}(AB \mid \alpha, \beta) + \mathbb{E}(AB' \mid \alpha, \beta') - \mathbb{E}(A'B \mid \alpha', \beta) + \mathbb{E}(A'B' \mid \alpha', \beta')$$

where $\mathbb{E}(AB \mid \alpha, \beta)$ means that Alice chooses the basis α and Bob chooses the basis β to measure their value. Note that we must estimate the terms one by one: Alice cannot measure both $A \mid \alpha$ and $A' \mid \alpha'$ at once, since doing a measurement modifies the state.

We want to test the quantum theories, so we consider another possible explanation. In this one, we say that the measurement in a lab does not impact the measurement in the other lab; but, in fact that, when creating the Bell state, both q-bit registered a same value λ (a "hidden variable") that they use when we measure them. This λ is given to these q-bits randomly when entangling them, following a PDF $h(\lambda)$. Mathematically, the fact that the measure only depends on λ means that:

$$\mathbb{P}(A = a, B = b \mid \lambda) = \mathbb{P}(A = a \mid \lambda)\mathbb{P}(B = b \mid \lambda)$$

In this case, we have:

$$|x| \leq 2$$

This inequality is also named the CHSH inequality.

If we consider the usual quantum theories, we can choose $\alpha, \beta, \alpha', \beta'$ such that:

$$x = 2\sqrt{2}$$

Measuring x experimentally, we can get that $x = 2\sqrt{2}$, showing that the theory of hidden variables does not hold physically. More specifically, it shows that the locality assumption we took is not correct: the measure in Alice's lab depends on the result of the measure in Bob's lab and inversely.

Remark Here, we measure A, B, A', B' using a Bell state. However, we can use an arbitrary state $|\psi\rangle$. This gives us that $|x| \leq 2$ is a necessary condition for a state to be a product state. Indeed, if it is a product state, then the locality assumption holds, and we are back in the classical inequality.

In fact, we can show that we can always find angles $\alpha, \beta, \alpha', \beta'$ such that $|x| > 2$ for an entangle state. This yields that if we can find some $\alpha, \beta, \alpha', \beta'$ where $|x| > 2$, then this necessarily yields that $|\psi\rangle$ is entangled. If however there exists no $\alpha, \beta, \alpha', \beta'$ where $|x| > 2$, then $|\psi\rangle$ is a product state.

This is named the Tsirelson bound.

Classical proof We begin by proving the inequality for the classical case.

For the simplicity of the notation, we will note $\mathbb{P}(A = a) = \mathbb{P}(a)$, and similarly for the other random variables.

We have that:

$$\begin{aligned}
\mathbb{E}(AB \mid \alpha, \beta) &= \sum_{a,b} ab\mathbb{P}(a, b \mid \alpha, \beta) \\
&= \int_{-\infty}^{\infty} d\lambda h(\lambda) \sum_{a,b} ab\mathbb{P}(a, b \mid \alpha, \beta, \lambda) \\
&= \int_{-\infty}^{\infty} d\lambda h(\lambda) \sum_{a,b} ab\mathbb{P}(a \mid \alpha, \lambda)\mathbb{P}(b \mid \beta, \lambda) \\
&= \int_{-\infty}^{\infty} d\lambda h(\lambda) \sum_{a} a\mathbb{P}(a \mid \alpha, \lambda) \sum_{b} b\mathbb{P}(b \mid \beta, \lambda) \\
&= \int_{-\infty}^{\infty} d\lambda h(\lambda)\mathbb{E}(A \mid \alpha, \lambda)\mathbb{E}(B \mid \beta, \lambda)
\end{aligned}$$

To again simplify the notation, we let $\mathbb{E}(A \mid \alpha, \lambda) = \hat{a}$ and similarly for the other terms. Doing the same reasoning for the other terms and putting everything together, we get:

$$\begin{aligned}
x &= \int_{-\infty}^{\infty} d\lambda h(\lambda)\left(\hat{a}\hat{b} + \hat{a}\hat{b}' - \hat{a}'\hat{b} + \hat{a}\hat{b}\right) \\
&= \int_{-\infty}^{\infty} d\lambda h(\lambda)\left[\hat{a}\left(\hat{b} + \hat{b}'\right) - \hat{a}'\left(\hat{b}' - \hat{b}\right)\right]
\end{aligned}$$

However, we notice that $\hat{a} = \mathbb{E}(A \mid \alpha, \lambda) \in \{-1, 1\}$: the value of A solely depends on the value of λ so, when we do our measurement in the basis α, we will always get the same value, which is either -1 or 1; and similarly for all other terms. We now want to use this fact to show that:

$$u = \hat{a}\left(\hat{b} + \hat{b}'\right) - \hat{a}'\left(\hat{b}' - \hat{b}\right) \in \{-2, 2\}$$

Indeed, we can consider two cases. If $\hat{b} = \hat{b}' \in \{-1, 1\}$, it yields that the second term is 0, and that the first term is either -2 or 2. If however, $\hat{b} \neq \hat{b}'$, it means that one is -1 and the other is 1, showing that the first term is 0. By the same reasoning, we get that $u \in \{-2, 2\}$.

All this yields that, using the triangle inequality:

$$|x| = \left|\int_{-\infty}^{\infty} d\lambda h(\lambda)u(\lambda)\right| \leq \int_{-\infty}^{\infty} d\lambda h(\lambda)|u(\lambda)| = 2\int_{-\infty}^{\infty} h(\lambda)d\lambda = 2$$

since this is a PDF. This gives our expected result.

Quantum proof We now prove the quantum equality.

When doing her measure in basis $|\alpha\rangle$, Alice uses the following operator:

$$\hat{A} = (+1)|\alpha\rangle\langle\alpha| + (-1)|\alpha_\perp\rangle\langle\perp|$$

We know how to compute expected values in the quantum realm, let us use this property:

$$\begin{aligned}
x = \langle B_{00}|\hat{A} \otimes \hat{B}|B_{00}\rangle &+ \langle B_{00}|\hat{A} \otimes \hat{B}'|B_{00}\rangle \\
- \langle B_{00}|\hat{A}' \otimes \hat{B}|B_{00}\rangle &+ \langle B_{00}|\hat{A}' \otimes \hat{B}'|B_{00}\rangle
\end{aligned}$$

Let us focus on $y = \langle B_{00}|A \otimes B|B_{00}\rangle$. We can use the following property of the Bell states:

$$|B_{00}\rangle = \frac{|\gamma\gamma\rangle + |\gamma_\perp\gamma_\perp\rangle}{\sqrt{2}}, \quad \forall\gamma$$

So:

$$\begin{aligned}
y = {} & \frac{\langle\alpha\alpha| + \langle\alpha_\perp\alpha_\perp|}{\sqrt{2}} \\
& \cdot \left(|\alpha\beta\rangle\langle\alpha\beta| - |\alpha_\perp\beta\rangle\langle\alpha_\perp\beta| - |\alpha\beta_\perp\rangle\langle\alpha\beta_\perp| + |\alpha_\perp\beta_\perp\rangle\langle\alpha_\perp\beta_\perp|\right) \\
& \cdot \frac{|\alpha\alpha\rangle + |\alpha_\perp\alpha_\perp\rangle}{\sqrt{2}} \\
= {} & \frac{1}{2}[2\langle\alpha|\beta\rangle\langle\beta|\alpha\rangle + 2\langle\alpha_\perp|\beta_\perp\rangle\langle\beta_\perp|\alpha_\perp\rangle] \\
= {} & \cos(\alpha-\beta)^2 - \sin(\alpha-\beta)^2 \\
= {} & \cos(2(\alpha-\beta))
\end{aligned}$$

We can do the same reasoning for the other terms and, putting everything together, we get:

$$x = \cos(2(\alpha-\beta)) + \cos(2(\alpha-\beta')) - \cos(2(\alpha'-\beta)) + \cos(2(\alpha'-\beta'))$$

Leaving $\alpha = 0$, $\alpha' = \frac{\pi}{4}$, $\beta = \frac{\pi}{8}$ and $\beta' = -\frac{\pi}{8}$, we finally get:

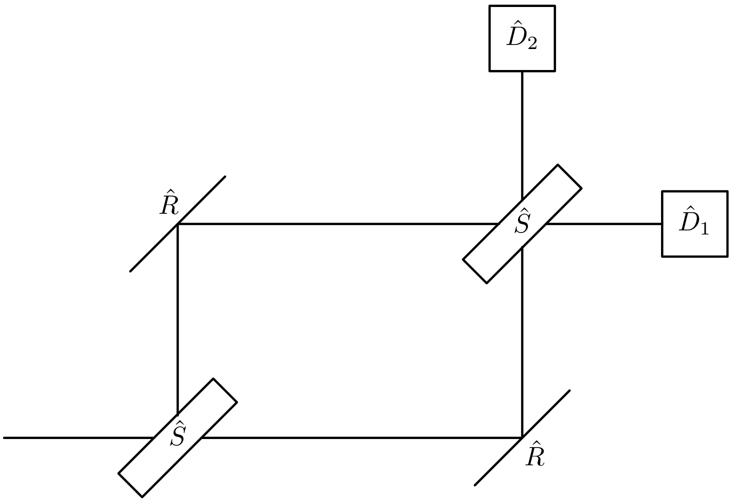
$$x = 4 \cdot \frac{\sqrt{2}}{2} = 2\sqrt{2}$$

ending our proof.

□

Mach-Zehnder interferometer

We consider an experiment where we have perfect mirrors $\hat{R}$ and semi-transparent mirrors $\hat{S}$ that let half of light go through. We construct the following experiment device:



There are two rays that merge to form the one that goes to the photodetector $\hat{D}_1$, and similarly for $\hat{D}_2$. We can construct this in a way that $\hat{D}_2$ receives no light because the waves interfere destructively; and $\hat{D}_1$ gets all the light because the waves interfere constructively.

Now, we send a single photon. However, we see that the photon manages to "interfere with itself": $\hat{D}_2$ will never see a photon, but $\hat{D}_1$ will always see one. This is however a unit of light, so it cannot have taken the two paths simultaneously. We have a problem with the classical description, we therefore need quantum. The quantum description was done in the first exercise series.

Spin precession

We consider a particle of spin-$\frac{1}{2}$ in a space with constant magnetic field $\vec{\boldsymbol{B}}$. We can make a physical analysis while making analogies with the classical case to know that the Hamiltonian is given by:

$$\hat{H} = -\gamma\frac{\hbar}{2}\vec{\boldsymbol{\sigma}} \bullet \vec{\boldsymbol{B}} = -\gamma\frac{\hbar}{2}\begin{pmatrix} B_z & B_x - iB_y \\ B_x + iB_y & -B_z \end{pmatrix}$$

Let us consider a magnetic field with only a $\hat{z}$ component, $\vec{\boldsymbol{B}} = \begin{pmatrix} 0 & 0 & B_0 \end{pmatrix}^T$:

$$\hat{H} = \begin{pmatrix} -\gamma\frac{\hbar}{2}B_0 & 0 \\ 0 & \gamma\frac{\hbar}{2}B_0 \end{pmatrix}$$

Then, we know that the solution to the Schrödinger's equation is:

$$\hat{U}(t) = \exp\left(-\frac{i}{\hbar}\hat{H}t\right) = \begin{pmatrix} \exp\left(\frac{it\gamma B_0}{2}\right) & 0 \\ 0 & \exp\left(\frac{-it\gamma B_0}{2}\right) \end{pmatrix}$$

where we used the fact that the exponential of a diagonal matrix is the exponential of the diagonal entries (this comes directly from the fact that that the exponential of a matrix has the same eigenkets but its eigenvalues are the exponential of the original ones).

Let us consider a starting state as its Bloch sphere representation:

$$|\psi(0)\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\varphi}|1\rangle$$

At time t, the state is given by:

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle = \exp\left(\frac{it\gamma B_0}{2}\right)\left(\cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i(\varphi - t\gamma B_0)}|1\rangle\right)$$

However, since the global phase does not matter, this is equivalent to:

$$|\psi(t)\rangle \equiv \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i(\varphi - t\gamma B_0)}|1\rangle$$

This yields that the state processes on the Bloch sphere around the $\hat{z}$ axis, at an angular frequency $\nu = \gamma B_0$. This is named the **Larmor frequency**.

This reasoning can be generalised to an arbitrary magnetic field $\vec{\boldsymbol{B}}$, which yields that the state precesses around the axis given by this vector $\vec{\boldsymbol{B}}$.

Remark In class, in lectures 5 and 6, we saw more complex examples with more complex non-constant Hamiltonians. This does not appear here, since this is pure computations, and it would thus be equivalent to reading the correction of the corresponding series.

However, as a general advice, it can often be useful to consider the fact that $\hat{A} \otimes \hat{B}$ and $\exp\left(\hat{A} \otimes \hat{B}\right)$ have the same eigenkets, which are the tensor products of the eigenkets of $\hat{A}$ and the ones of $\hat{B}$. Getting the eigenkets of the Hamiltonian solves Schrödinger's equation (as mentioned in the paragraph on this equation), so it might suffice to get the eigenkets of $\hat{A}$ and $\hat{B}$.

4 Communication protocols

Quantum key distribution

The goal of the **quantum key distribution** (QKD) protocol is to share a common secret between Alice and Bob, while making sure nobody else can have it too. This requires a classical and a quantum channel between them.

This goes in four phases:

1. Alice generates two IID strings uniformly at random of classical bits: $e_1, \dots, e_n$ and $x_1, \dots, x_n$. She sends n photons to Bob, in states:
$$|\psi_i\rangle = \hat{H}^{x_i}|e_i\rangle, \quad \hat{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$
where $\hat{H}$ is the Hadamard matrix.
2. Bob generates a IID string uniformly at random of classical bits $d_1, \dots, d_n$. If $d_i = 0$, he measures the corresponding photo $|\psi_i\rangle$ in the basis of σ_z, $\{|0\rangle, |1\rangle\}$; if $d_i = 1$, he measures it in the basis of σ_x, $\left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$. This gives him a sequence of classical bits $y_1, \dots, y_n$.
3. Alice and Bob reveal the choices of encoding and decoding basis $e_1, \dots, e_n$ and $d_1, \dots, d_n$; while keeping $x_1, \dots, x_n$ and $y_1, \dots, y_n$ secret. They get rid of all (x_i, y_i) where $e_i \neq d_i$, and keep all the others. Those bits are the same for Alice and Bob, i.e. $\mathbb{P}(x_i = y_i \mid e_i = d_i) = 1$; this is a shared secret of expected size $\frac{n}{2}$ that can for instance be used as one-time pad.
4. Alice and Bob finally need to do a security check. They sacrifice a small part of their shared secret, $s = \varepsilon\frac{n}{2}$ where $\varepsilon \ll 1$ is very small. They verify that the number of bits that are equal is approximately s. Otherwise, there was a lot of noise or an eavesdropper.

Shared secret proof

To show that this protocol indeed yields a shared secret, we need to show that:
$$\mathbb{P}(x_i = y_i \mid e_i = d_i) = 1, \quad \mathbb{P}(x_i = y_i \mid e_i \neq d_i) = \frac{1}{2}$$

Now, we know that the probability to go from $H^{e_i}|x_i\rangle$ (the state sent by Alice) to $H^{d_i}|y_i\rangle$ (the state after Bob's measure) is, by Born's rule:
$$\mathbb{P}(x_i = y_i \mid e_i, d_i) = \left|\langle y_i|\left(\hat{H}^{d_i}\right)^\dagger \hat{H}^{e_i}|x_i\rangle\right|^2 = \left|\langle y_i|\hat{H}^{d_i+e_i}|x_i\rangle\right|$$

where we used the fact that the Hadamard matrix is hermitian.

We moreover know that $\hat{H}^2 = \hat{I}$. This means that, for any $e_i, d_i \in \{0, 1\}$ such that $e_i = d_i$, we always have that $\hat{H}^{e_i+d_i} = \hat{I}$. This yields:
$$\mathbb{P}(x_i = y_i \mid e_i = d_i) = |\langle y_i|x_i\rangle|^2 = \begin{cases} 1, & \text{if } x_i = y_i \\ 0, & \text{otherwise} \end{cases}$$

Now, when $e_i \neq d_i$, we always have $\hat{H}^{e_i+d_i} = \hat{H}$. This gives us:
$$\mathbb{P}(x_i = y_i \mid e_i \neq d_i) = \left||y_i\rangle\hat{H}|x_i\rangle\right|^2 = \left|\langle y_i|\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_i})|1\rangle\right|^2 = \frac{1}{2}$$

as required.

Eavesdropper detection proof

We now want to show that we are able to correctly detect eavesdroppers. They can never copy the state because of the no-cloning theorem, so the only thing they can do is observe the q-bits in some basis.

Let's say that Eve follows what Bob does, generating a random IID string uniformly at random $E_1, \ldots, E_n$ and using it to measure in the $\hat{\sigma}_z$ or $\hat{\sigma}_x$ basis. She then sends the q-bits to Bob so that he does not know Eve looked at the q-bits. In this case, we have:

$$\begin{aligned}
&\mathbb{P}(x_i = y_i \mid e_i = d_i) \\
&= \mathbb{P}(x_i = y_i \mid e_i = d_i, E_i = e_i)\mathbb{P}(E_i = e_i \mid e_i = d_i) \\
&\quad + \mathbb{P}(x_i = y_i \mid e_i = d_i, E_i \neq e_i)\mathbb{P}(E_i \neq e_i \mid e_i = d_i) \\
&= \mathbb{P}(x_i = y_i \mid E_i = e_i)\mathbb{P}(E_i = e_i) + \mathbb{P}(x_i = y_i \mid E_i \neq e_i)\mathbb{P}(E_i \neq e_i) \\
&= 1 \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} \\
&= \frac{3}{4}
\end{aligned}$$

since, in the first case, Eve did not change the state; but, in the second, she changed it to a wrong superposition due to her measurement.

We have $\mathbb{P}(x_i = y_i \mid e_i = d_i) < 1$, so Alice and Bob will notice that there is an issue in the fourth phase.

Teleportation

The goal of the **teleportation** protocol is to send an arbitrary q-bit to Bob, using a pre-shared Bell state split between the two and two bits sent over a classical channel.

In other words, the starting state is $|\psi\rangle_{123} = |\varphi\rangle_1 \otimes |B_{00}\rangle_{23}$, where the two first q-bits belong to Alice, and the third q-bit (the second half of the Bell state) belongs to Bob. The goal is to end up with something of the form $|\text{something}\rangle_{12} \otimes |\varphi\rangle_3$.

This goes in two phases:

1. Alice measures in the Bell state basis her two q-bits. She sends the value $v \in \{00, 01, 10, 11\}$ measured to Bob.
2. According to the value Bob receives, he can apply a unitary operation on his q-bit $|\varphi'\rangle$ to get $|\varphi\rangle$:

$$|\varphi\rangle = \begin{cases} |\varphi'\rangle, & \text{if } v = 00 \\ \hat{\sigma}_X|\varphi'\rangle, & \text{if } v = 01 \\ \hat{\sigma}_Z|\varphi'\rangle, & \text{if } v = 10 \\ i\hat{\sigma}_Y|\varphi'\rangle, & \text{if } v = 11 \end{cases}$$

Proof

The state Alice wants to send is $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ for some $\alpha, \beta \in \mathbb{C}$. This yields that the total state before any measurement is:

$$\begin{aligned}
|\psi\rangle &= |\varphi\rangle \otimes |B_{00}\rangle \\
&= (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\
&= \frac{\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle}{\sqrt{2}}
\end{aligned}$$

We only prove that this result is correct when Alice gets $v = 01$ after her measurement, the other cases are similar.

Since Alice measured $v = 01$, it means the first two q-bits collapsed to:

$$|B_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

By the theory of partial measurements, after her measurement, the total state is proportional to:

$$\begin{aligned} c|\psi'\rangle &= \left(|B_{01}\rangle\langle B_{01}| \otimes \hat{I}\right)|\psi\rangle \\ &= \left(\frac{|01\rangle\langle 01| + |10\rangle\langle 01| + |01\rangle\langle 10| + |10\rangle\langle 10|}{2} \otimes \hat{I}\right) \\ &\quad \cdot \frac{\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle}{\sqrt{2}} \end{aligned}$$

The maths here is not particularly hard, but we have to be careful to handle not to make a mistake. We for instance have:

$$\left(|10\rangle\langle 01| \otimes \hat{I}\right)|abc\rangle = |10\rangle\langle 01|ab\rangle \otimes \hat{I}|c\rangle = \begin{cases} |10c\rangle, & \text{if } ab = 01 \\ 0, & \text{otherwise} \end{cases}$$

This yields us that:

$$\begin{aligned} c|\psi'\rangle &= \frac{\alpha|011\rangle + \alpha|101\rangle + \beta|010\rangle + \beta|100\rangle}{2\sqrt{2}} \\ &= \frac{1}{2}\frac{|01\rangle + |10\rangle}{\sqrt{2}} \otimes (\alpha|1\rangle + \beta|0\rangle) \\ &= \frac{1}{2}|B_{01}\rangle \otimes |\varphi'\rangle \end{aligned}$$

Now, to get φ back, Bob can do:

$$\hat{\sigma}_X|\varphi'\rangle = \alpha\hat{\sigma}_X|1\rangle + \beta\hat{\sigma}_X|0\rangle = \alpha|0\rangle + \beta|1\rangle = |\varphi\rangle$$

The other cases are completely similar.

□

Dense coding

The goal of the **dense coding** protocol is to send two classical bits to Bob, using a pre-shared Bell state split between the two and a quantum channel.

This goes in two phases:

1. Depending on the value $v \in \{00, 01, 10, 11\}$ Alice wants to send, she applies a unitary operation $\hat{U}_A$ on her q-bit:

$$\hat{U}_A = \begin{cases} \hat{I}, & \text{if } v = 00 \\ \hat{\sigma}_x, & \text{if } v = 01 \\ \hat{\sigma}_z, & \text{if } v = 10 \\ \hat{\sigma}_x\hat{\sigma}_z, & \text{if } v = 11 \end{cases}$$

   She then sends her q-bit to Bob.
2. Bob measures the two q-bit using the Bell state basis. The value measured is v.

Proof

The starting state is the first Bell state:

$$|\psi\rangle = |B_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

We only consider the case where $v = 01$, the other cases are similar. This means that Alice applies a unitary operation $\hat{U}_A = \hat{\sigma}_x$, yielding that the new state is:

$$|\psi'\rangle = \left(\hat{U}_A \otimes \hat{I}\right)|\psi\rangle = \left(\hat{\sigma}_x \otimes \hat{I}\right)\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$\hat{\sigma}_x$ has the effect of flipping the bit it acts on, so:

$$|\psi'\rangle = \frac{|10\rangle + |01\rangle}{\sqrt{2}} = |B_{01}\rangle$$

When Bob measures $|\psi'\rangle$, he will indeed get $v = 01$. The other cases are completely similar.

□

5 Density matrices and information theory

Density matrix A matrix $\hat{\rho}$ is named a **density matrix** if it has the following properties:

1. It is hermitian.
2. It is positive semi-definite.
3. $\mathrm{Tr}(\hat{\rho}) = 1$.

Remark This is a generalisation of the concept of quantum states. Indeed, if we have a state $|\psi\rangle$, then we can always form the following density matrix:

$$\hat{\rho} = |\psi\rangle\langle\psi|$$

If $\hat{\rho}$ can be written in this form, it is named a **pure state**. This must not be mistaken with entangled states: if ψ is entangled, $\hat{\rho}$ is also a pure state. States that are not pure states are **mixed states**.

Intuition Since $\hat{\rho}$ is hermitian, we can find an orthonormal basis $|\varphi_i\rangle$ of real eigenvalues p_i:

$$\hat{\rho} = \sum_{i=1}^{n} p_i |\varphi_i\rangle\langle\varphi_i|$$

The fact that it is positive semi-definite tells us that $p_i \geq 0$ for all i. The fact that the trace is 1 tells us that $p_1 + \ldots + p_n = 1$. Those p_i can therefore be interpreted as some form of probabilities.

This yields the following concept.

Statistical mixture A system that is a **statistical mixture** of pure states can be represented using a density matrix. Let's say that it has a fraction p_i of state $|\varphi_i\rangle$ (for $i \in \{1, \ldots, k\}$), where $p_1 + \ldots + p_k = 1$. In other words, if we consider a random particle inside the statistical mixture, it has state $|\varphi_i\rangle$ with probability p_i.

Then the density matrix of this statistical mixture is given by:

$$\hat{\rho} = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|$$

This indeed has the three properties of a density matrix.

Remark This situation is the best way to get intuition about a density matrix. Given a density matrix $\hat{\rho}$, one can diagonalise it to see what statistical mixture would yield this $\hat{\rho}$. We can then interpret our system as a box where, when we look inside, we get state $|\varphi_i\rangle$ with probability p_i.

Expected value The expected value of an observable $\hat{A}$ (of eigenkets $|A_i\rangle$ and eigenvalues a_i) over a state represented by a density matrix $\hat{\rho}$ is given by:

$$\left\langle \hat{A} \right\rangle = \mathrm{Tr}\left(\hat{\rho}\hat{A}\right)$$

Mnemonic

We can recall this formula by seeing the trace as a sum, $\hat{\rho}$ as probabilities and $\hat{A}$ as values. This is then completely analogous to random variables:

$$\mathbb{E}(X) = \sum_i p_i X_i$$

Implication

This means that the expected value of an observable $\hat{A}^p$ under the state $\hat{\rho}$ is:

$$\left\langle \hat{A}^p \right\rangle = \operatorname{Tr}\left(\hat{\rho}\hat{A}^p\right)$$

We moreover know that $\operatorname{Var}(X) = \mathbb{E}\left(X^2\right) - \mathbb{E}(X)^2$. This means that the variance of our observable over the state $\hat{\rho}$ is:

$$\left\langle \hat{A}^2 \right\rangle - \left\langle \hat{A} \right\rangle^2 = \operatorname{Tr}\left(\hat{\rho}\hat{A}^2\right) - \operatorname{Tr}\left(\hat{\rho}\hat{A}\right)^2$$

Pure state

Let us verify this makes sense for a pure state $\hat{\rho} = |\psi\rangle\langle\psi|$. By the cyclicity of the trace, we have:

$$\left\langle \hat{A} \right\rangle = \operatorname{Tr}\left(\hat{\rho}\hat{A}\right) = \operatorname{Tr}\left(|\psi\rangle\langle\psi|\hat{A}\right) = \operatorname{Tr}\left(\langle\psi|\hat{A}|\psi\rangle\right) = \langle\psi|\hat{A}|\psi\rangle$$

since $\operatorname{Tr}(a) = a$ for any $a \in \mathbb{C}$.
This is indeed the result we got for pure states.

Proof

We know that we can always diagonalise $\hat{A}$ and $\hat{\rho}$:

$$\hat{A} = \sum_i a_i |A_i\rangle\langle A_i|, \quad \hat{\rho} = \sum_j p_j |\varphi_j\rangle\langle\varphi_j|$$

When measuring something in this statistical mixture with our observable, we will get a random sate $|\varphi_j\rangle$ with probability p_j. By the Born rule, this state then collapses to $|A_i\rangle$ with probability $|\langle A_i|\varphi_j\rangle|^2$, outputting a value a_i to the measure instrument. We therefore have:

$$\begin{aligned}
\sum_i a_i \mathbb{P}(\text{measure } a_i) &= \sum_i a_i \sum_j |\langle A_i|\varphi_j\rangle|^2 \mathbb{P}(\text{chose } \varphi_j) \\
&= \sum_i \sum_j a_i p_j \langle\varphi_j|A_i\rangle\langle A_i|\varphi_j\rangle \\
&= \sum_j p_j \langle\varphi_j| \left(\sum_i a_i |A_i\rangle\langle A_i| \right) |\varphi_j\rangle \\
&= \sum_j p_j \langle\varphi_j|\hat{A}|\varphi_j\rangle
\end{aligned}$$

where we recognised the diagonal representation of $\hat{A}$ in its eigenbasis.
However, by definition of eigenvalues:

$$p_j \langle\varphi_j| = \langle\varphi_j| p_j = \langle\varphi_j|\hat{\rho}^\dagger = \langle\varphi_j|\hat{\rho}$$

This yields:

$$\sum_i a_i \mathbb{P}(\text{measure } a_i) = \sum_j \langle\varphi_j|\hat{\rho}A|\varphi_j\rangle = \operatorname{Tr}(\hat{\rho}A)$$

as *expected.*

□

Non-isolated system A non-isolated system S can also be represented using a density matrix. To do so, we need to find its environment E such that $S \cup E$ is isolated. By regular quantum physics, a state in $\mathcal{H}_S \otimes \mathcal{H}_E$ is always pure since this system is isolated. The density matrix of $S \cup E$ is therefore easily found:

$$\hat{\rho}_{SE} = |\psi\rangle\langle\psi|$$

To get the density matrix of S, we then use a partial trace:

$$\hat{\rho}_S = \operatorname{Tr}_{\mathcal{H}_E}(\hat{\rho}_{SE})$$

Remark For this to make sense with the previous theorem, we require that, for any observable $\hat{A}$ in $\mathcal{H}_S$, its expected value must be given by $\operatorname{Tr}_{\mathcal{H}_S}\left(\hat{A}\hat{\rho}_S\right)$. Indeed, considering the whole system $\mathcal{H}_S \otimes \mathcal{H}_E$, we do have:

$$\left\langle \hat{A} \otimes \hat{I}_E \right\rangle = \operatorname{Tr}\left(\hat{\rho}_{SE}\hat{A} \otimes \hat{I}_E\right) = \operatorname{Tr}_{\mathcal{H}_S}\left(\hat{\rho}_S\hat{A}\right)$$

as expected.

Bloch ball The density matrix $\hat{\rho}$ of one q-bit (meaning that it is 2×2) can be represented as:

$$\hat{\rho} = \frac{1}{2}\left(\hat{I} + \vec{\boldsymbol{a}} \bullet \vec{\hat{\boldsymbol{\sigma}}}\right)$$

where the vector $\vec{\boldsymbol{a}} \in \mathbb{R}^3$ is such that:

$$\|\vec{\boldsymbol{a}}\| \leq 1$$

Interpretation This means that we can always represent a density matrix on a ball (a filled sphere). A state is on the surface if and only if it is pure; and, in this case, it behaves just like the Bloch sphere. A state that is in the centre is a Bernoulli random variable that gives $|0\rangle$ or $|1\rangle$ both with probability $\frac{1}{2}$. Any state in between is a mix of the two.

Proof It is possible to show that $\left(\hat{I}, \hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z\right)$ form an orthonormal basis for 2×2 matrices. Therefore, we can always express a 2×2 matrix as:

$$\hat{\rho} = a_0\hat{I} + a_1\hat{\sigma}_x + a_2\hat{\sigma}_y + a_3\hat{\sigma}_z$$

We know that $\operatorname{Tr}(\hat{\rho}) = 1$, thus:

$$\begin{aligned}1 &= a_0 \operatorname{Tr}\left(\hat{I}\right) + a_1 \operatorname{Tr}(\hat{\sigma}_x) + a_2 \operatorname{Tr}(\hat{\sigma}_y) + a_3 \operatorname{Tr}(\hat{\sigma}_z) \\ &= a_0 \cdot 2 + a_1 \cdot 0 + a_2 \cdot 0 + a_3 \cdot 0 \\ &= 2a_0\end{aligned}$$

which yields that $a_0 = \frac{1}{2}$.

We now leave $a_x = 2a_1$, $a_y = 2a_2$ and $a_z = 2a_3$ in order to simplify the notations. So far, we got that we can write:

$$\hat{\rho} = \frac{1}{2}\left(\hat{I} + a_x\hat{\sigma}_x + a_y\hat{\sigma}_y + a_z\hat{\sigma}_z\right)$$

We only need to show that $\|\vec{\boldsymbol{a}}\| \leq 1$. To do so, we can compute the determinant. We know that it is positive: it is equal to the product of the eigenvalues, which are positive since density matrices are positive semi-definite. This gives us:

$$\begin{aligned} 0 \leq\ & \det(\hat{\rho}) \\ =\ & \frac{1}{4}\left(\det\left(\hat{I}\right) + a_x^2 \det(\hat{\sigma}_x) + a_y^2 \det(\hat{\sigma}_y) + a_z^2 \det(\hat{\sigma}_z)\right) \\ =\ & \frac{1}{4}(1 - a_x^2 - a_y^2 - a_z^2) \\ =\ & \frac{1}{4}\left(1 - \|\vec{\boldsymbol{a}}\|^2\right) \end{aligned}$$

We indeed get that $\|\vec{\boldsymbol{a}}\| \leq 1$.

□

Von Neumann entropy The **Von Neumann (quantum) entropy** of a density matrix $\hat{\rho}$ is given by:

$$S(\hat{\rho}) = -\operatorname{Tr}(\hat{\rho}\ln(\hat{\rho}))$$

Intuition We know that the trace is the sum of eigenvalues. The eigenvalues of $\hat{\rho}\ln(\hat{\rho})$ are $p_i \ln(p_i)$ (where the p_i are the eigenvalues of $\hat{\rho}$). This yields that:

$$S(\hat{\rho}) = -\sum_i p_i \ln(p_i)$$

where we use the continuity extension $0 \cdot \ln(0) \overset{\text{def}}{=} 0$.
This is completely analogous to the classical Shannon entropy.

Property 1 For a Hilbert space of dimension d, we have:

$$0 \leq S(\hat{\rho}) \leq \ln(d)$$

We moreover have $S(\hat{\rho}) = 0$ if an only if $\hat{\rho}$ is a pure state, and $S(\hat{\rho}) = \ln(d)$ if and only if $\hat{\rho} = \frac{1}{d}\hat{I}$.

Property 2 The entropy has the subadditivity property:

$$S(\hat{\rho}_{AB}) \leq S(\hat{\rho}_A) + S(\hat{\rho}_B)$$

Property 3 Given a density matrix representing a q-bit, $\hat{\rho} = \frac{1}{2}\left(\hat{I} + \vec{\boldsymbol{a}} \bullet \vec{\hat{\boldsymbol{\sigma}}}\right)$, its entropy is given by:

$$S(\hat{\rho}) = -\frac{1 + \|\vec{\boldsymbol{a}}\|}{2}\ln\left(\frac{1 + \|\vec{\boldsymbol{a}}\|}{2}\right) - \frac{1 - \|\vec{\boldsymbol{a}}\|}{2}\ln\left(\frac{1 - \|\vec{\boldsymbol{a}}\|}{2}\right)$$

This can be found directly by solving the following equation, that gives us the eigenvalues p_1 and p_2 of $\hat{\rho}$:

$$\begin{cases} p_1 p_2 = \det(\hat{\rho}) = \frac{1}{4}\left(1 - \|\vec{\boldsymbol{a}}\|^2\right) \\ p_1 + p_2 = \operatorname{Tr}(\hat{\rho}) = 1 \end{cases}$$

We then simply have:

$$S(\hat{\rho}) = -p_1 \ln(p_1) - p_2 \ln(p_2)$$

Schmidt theorem If a statistical mixture $\hat{\rho}_{AB}$ is pure, i.e. $\hat{\rho}_{AB} = |\psi\rangle\langle\psi|$, then $\hat{\rho}_A$ and $\hat{\rho}_B$ have the same eigenvalues with same multiplicity.
This notably implies that:

$$S(\hat{\rho}_A) = S(\hat{\rho}_B)$$

This value is named the **entanglement entropy** of $|\psi\rangle$.

Example

Let us consider a Bell state in $\mathcal{H}_A \otimes \mathcal{H}_B$:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

The density matrix in the whole Hilbert space is given by:

$$\hat{\rho}_{AB} = |\psi\rangle\langle\psi| = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$$

We notice that, using properties of the partial trace:

$$\mathrm{Tr}_B(|ab\rangle\langle cd|) = |a\rangle\langle c|\,\mathrm{Tr}(|b\rangle\langle d|) = |a\rangle\langle c|\langle d|b\rangle$$

Then, the density matrix in the Hilbert space $\mathcal{H}_A$ is:

$$\begin{aligned}
\hat{\rho}_A = {} & \mathrm{Tr}_B(\hat{\rho}_{AB}) \\
= {} & \frac{1}{2}(|0\rangle\langle 0|\langle 0|0\rangle + |0\rangle\langle 1|\langle 1|0\rangle + |1\rangle\langle 0|\langle 0|1\rangle + |1\rangle\langle 1|\langle 1|1\rangle) \\
= {} & \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \\
= {} & \frac{1}{2}\hat{I}
\end{aligned}$$

This is the 2 × 2 matrix that has maximum entropy, telling us that this Bell state has maximal entanglement entropy, $\ln(2)$.

We can do the same reasoning on the following state, which would have 0 entanglement entropy since it is a product sate:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$