5 Multiple 2-state systems

A single 2-state system was referred to as a single q-bit and could corresponds to a spin-$\frac{1}{2}$. We now want to study systems of multiple q-bits or multiple spin-$\frac{1}{2}$. We will begin by considering two q-bits or two spin-$\frac{1}{2}$. Physically, a system of two spin-$\frac{1}{2}$ is realised for example by the spin of the proton and the spin of the electron in the hydrogen atom and the coupling of these two spins (the energy of the magnetic moment of the electron in the magnetic field created by the magnetic moment of the proton) gives rise to the so-called hyperfine structure of the hydrogen atom. The wavelength/frequency corresponding to the transition between the two energy levels is of utmost importance in astronomy because hydrogen is omnipresent in the universe and is precisely detected via this 21 cm wave-length. Moreover, the frequency of this transition has been measured to an extremely high precision and even slight frequency shifts can be measured and then interpreted (e.g. as due to Doppler shifts caused by moving clouds of hydrogen).

It is important that the different 2-state systems can be considered as distinguishable, and clearly labelled as system 1 and system 2. This is the case for the spin of the electron and the spin of the proton. It is also the case for the spins of two atoms at well defined positions 1 and 2 in a crystal. Indeed, as we will see later, if the two systems (particles) are indistinguishable the total state must be either symmetric (bosons) or anti-symmetric (fermions) under the exchange of 1 and 2. If 1 and 2 are distinguishable we will not need to deal with this subtlety.

5.1 Tensor product : definition, factorised and entangled states

Suppose now we have two distinct 2-state systems. We will label them by 1 and 2. We pick a basis for the first system which we label $\{|1:+\rangle, |1:-\rangle\}$ and similarly a basis for the second system $\{|2:+\rangle, |2:-\rangle\}$. Let us use the language of spin-$\frac{1}{2}$, and suppose that $\{|1:+\rangle, |1:-\rangle\}$ are the eigenvectors of $S_z^{(1)}$. To be very clear, this means that if the first spin is $|1:\pm\rangle$ and we measure its spin in the z direction we find $\pm\frac{\hbar}{2}$ with probability one. Said differently, the $|1:\pm\rangle$ are eigenstates of the observable $S_z^{(1)}$. Similarly, for the second spin, the $|2:\pm\rangle$ are eigenstates of the observable $S_z^{(2)}$ and if we measure the second spin in the z direction we find $\pm\frac{\hbar}{2}$ with probability one.

Since the two particles (spins) are different and distinguishable, the combined system will have four possible basis states corresponding to the measurement of the first spin in the z-direction and of the second spin in the z-direction giving $(\frac{\hbar}{2}, \frac{\hbar}{2})$ or $(\frac{\hbar}{2}, -\frac{\hbar}{2})$ or $(-\frac{\hbar}{2}, \frac{\hbar}{2})$ or $(-\frac{\hbar}{2}, -\frac{\hbar}{2})$. We can then denote these basis states as $|1:+;2:+\rangle, |1:+;2:-\rangle, |1:-,2:+\rangle, |1:-;2:-\rangle$.

We could also denote these same basis states as $|1:+\rangle\,|2:+\rangle$, $|1:+\rangle\,|2:-\rangle$, etc. This writing looks like we are taking a "product" of two kets. This can be made more precise mathematically as a tensor product of a vector (ket) of the first Hilbert space with a vector (ket) of the second Hilbert space. The correct notation then is $|1:+\rangle \otimes |2:+\rangle$, $|1:+\rangle \otimes |2:-\rangle$, etc. But this is just a fancy notation, and our previous $|1:+;2:+\rangle$, $|1:+;2:-\rangle$, etc, is (almost) just as good. We will often use an even simpler notation, namely $|++\rangle$, $|+-\rangle$, etc with the understanding that the

first label refers to the first particle and the second label to the second. We will use the different notations interchangeably, trying to reconcile simplicity, clarity and being non-ambiguous.

Here is the mathematical definition of tensor product :

Definition : The tensor product $V \otimes W$ of two vector spaces V and W (over the same field) is a vector space to which is associated a bilinear map $V \times W \to V \otimes W$ that maps a pair $(v, w),\ v \in V,\ w \in W$ to an element of $V \otimes W$ denoted $v \otimes w$.

The important notions are the bilinearity, which means linear in the first factor *and* linear in the second, so that

$$(av_1 + bv_2) \otimes (cw_1 + dw_2) = ac\, v_1 \otimes w_1 + ad\, v_1 \otimes w_2 + bc\, v_2 \otimes w_1 + bd\, v_2 \otimes w_2 \ , \tag{5.1}$$

and the fact that $V \otimes W$ is a vector space which means that it contains *any* linear combinations like $\alpha v_1 \otimes w_1 + \beta v_2 \otimes w_2$ even if they cannot be written as a single "factorised" term $v \otimes w$.

Here is a physically relevant example where we use the linearity. Suppose we want to change the basis for the first particle and express $|+\rangle \equiv |+\rangle_z$ as $\frac{1}{\sqrt{2}}(|+\rangle_x + |-\rangle_x)$. Then the tensor product notation allows us to follow through this change as

$$|1:+\rangle_z \otimes |2:+\rangle_z = \frac{1}{\sqrt{2}}\big(\,|1:+\rangle_x + |1:-\rangle_x\,\big) \otimes |2:+\rangle_z = \frac{1}{\sqrt{2}}\big(\,|1:+\rangle_x \otimes |2:+\rangle_z + |1:-\rangle_x \otimes |2:+\rangle_z\,\big) \tag{5.2}$$

where we obviously used the linearily in the last step. Of course, we can rewrite this in any of our other notations, provided we indicate which basis (z or x) is use, e.g. as $|1:+_z; 2:+_z\rangle = \frac{1}{\sqrt{2}}\big(\,|1:+_x; 2:+_z\rangle + |1:-_x; 2:+_z\rangle\,\big)$, but it would be less convenient to indicate the intermediate step in this notation.

Note that our combined system consisting of two 2-state systems has 4 basis states because $4 = 2 \times 2$ and not because $4 = 2 + 2$. If we combined two 3-state systems, there would be $3 \times 3 = 9$ basis states. More generally, if $\{|1:a\rangle\,, a = 1, \dots N_1\}$ is a basis of a first N_1-state system and $\{|2:b\rangle\,, b = 1, \dots N_2\}$ a basis of a second N_2-state system, a basis for the combined system is $\{|1:a\rangle \otimes |2:b\rangle\,,\ a = 1, \dots N_1,\ b = 1, \dots N_2\}$ and contains $N_1 \times N_2$ basis vectors. If $\mathcal{H}_{(1)}$ is a first Hilbert space of dimension N_1 and $\mathcal{H}_{(2)}$ is a second Hilbert space of dimension N_2, their tensor product $\mathcal{H}_{(1)} \otimes \mathcal{H}_{(2)}$ is a Hilbert space of dimension $N_1 N_2$. Again, this tensor product space contains all possible (complex) linear combinations of the $N_1 N_2$ basis vectors. Let us insist that such a general state is *not* of the form $|\psi_1\rangle \otimes |\phi_2\rangle$ with $|\psi_1\rangle \in \mathcal{H}_{(1)}$ and $|\phi_2\rangle \in \mathcal{H}_{(2)}$. Indeed, a general state in $\mathcal{H}_{(1)}$ depends on the N_1 complex coefficients of $|\psi_1\rangle$ with respect to the N_1 basis vectors. But the overall normalisation and phase are irrelevant (we are really dealing with the rays), so there are only $N_1 - 1$ relevant complex coefficients. Similarly for $|\phi_2\rangle$ there are $N_2 - 1$ relevant complex coefficients. Then the factorised state $|\psi_1\rangle \otimes |\phi_2\rangle$ depends on $N_1 - 1 + N_2 - 1 = N_1 + N_2 - 2$ relevant complex oefficients. On the other hand a general state in the product Hilbert space $\mathcal{H}_{(1)} \otimes \mathcal{H}_{(2)}$ has $N_1 N_2$ complex expansion coefficients on the $N_1 N_2$ basis vectors , which are $N_1 N_2 - 1$ relevant complex coefficients. Now, for $N_1, N_2 \geq 2$ we always have $N_1 N_2 - 1 > N_1 + N_2 - 2$ since this is

equivalent to $(N_1-1)(N_2-1)>0$ which is obviously true. Hence, $\mathcal{H}_{(1)}\otimes\mathcal{H}_{(2)}$ always contains states that cannot be written as $|\psi_1\rangle\otimes|\phi_2\rangle$.

Definition : A state in the tensor product space $\mathcal{H}_{(1)}\otimes\mathcal{H}_{(2)}$ that can be written as $|\psi_1\rangle\otimes|\phi_2\rangle$ is called a *factorised* state, and a state that *cannot* be written in this form is called an *entangled* state.

We want our tensor product space to be a Hilbert space again (as we already implicitly assumed). This requires the definition of a hermitian inner product. Requiring that this hermitian product is linear in the second factor and anti-linear in the first, it is enough to define it between the basis states. The natural definition is of course

$$\big(\,\langle 1:a|\otimes\langle 2:b|\,\big)\big(\,|1:c\rangle\otimes|2:d\rangle\,\big)=\langle 1:a\,|1:c\rangle\;\langle 2:b\,|2:d\rangle\;\;. \tag{5.3}$$

Then, in particular, the inner product between factorised states is $\big(\,\langle\psi_1|\otimes\langle\phi_2|\,\big)\big(\,|\chi_1\rangle\otimes|\eta_2\rangle\,\big)=\langle\psi_1\,|\chi_2\rangle\;\langle\phi_2\,|\eta_2\rangle$. But again, the hermitian inner product is more generally defined by (5.3) and the linearity and anti-linearity.

Multiple 2-state systems : Instead of just considering two spin-$\frac{1}{2}$ systems one can, of course, consider N such systems and then the corresponding Hilbert space will be the N-fold tensor product of the Hilbert space of a single spin-$\frac{1}{2}$. Its dimension is 2^N and a basis is e.g. the set of all $|1:a_1\rangle\otimes|2:a_2\rangle\otimes\ldots\otimes|N:a_n\rangle$ where each a_i can be either $+$ or $-$. More generally, one defines the tensor product of N (finite-dimensional) Hilbert spaces $\mathcal{H}_{(i)},\;i=1,\ldots N$ of dimensions d_i, denoted $\mathcal{H}_{(1)}\otimes\mathcal{H}_{(2)}\otimes\ldots\otimes\mathcal{H}_{(N)}$. Its dimension is $\prod_{i=1}^N d_i$. If $\{|i:a^{(i)}_{n_i}\rangle_{n_i=1,\ldots d_i}\}$ is a basis of $\mathcal{H}_{(i)}$ then the set of all $|1:a^{(1)}_{i_1}\rangle\otimes|2:a^{(2)}_{i_2}\rangle\otimes\ldots\otimes|N:a^{(N)}_{i_N}\rangle$ constitutes a basis for the tensor product Hilbert space.

5.2 Linear operators on $\mathcal{H}_{(1)}\otimes\mathcal{H}_{(2)}$

Of course, linear operators on the tensor product space $\mathcal{H}_{(1)}\otimes\mathcal{H}_{(2)}$ are defined in the same way as on any (finite-dimensional) Hilbert space. By linearity, any linear operator is determined by its action on the N_1N_2 basis vectors $|1:a\rangle\otimes|2:b\rangle$. This means that the matrix corresponding to a linear operator is an $N_1N_2\times N_1N_2$ matrix consisting of $N_1^2N_2^2$ matrix elements. Already for $N_1=N_2=2$ these are 4×4 matrices with 16 matrix elements. Again, these are many more possibilities than one gets by combining just the 4 matrix elements of a linear operator on $\mathcal{H}_{(1)}$ with the 4 matrix elements of a linear operator on $\mathcal{H}_{(2)}$. Nevertheless, an interesting subclass of all linear operators on $\mathcal{H}_{(1)}\otimes\mathcal{H}_{(2)}$ are precisely those that are made from the individual linear operators on the individual Hilbert spaces.

Let us begin by considering the Hamiltonian and energy. Let H_1 be the Hamiltonian of the first system and H_2 the Hamiltonian for the second system and let $|\varphi^{(1)}_a\rangle$ and $|\varphi^{(2)}_b\rangle$ be their eigenstates with eigenvalues $E^{(1)}_a$ and $E^{(2)}_b$:

$$H_1\,|\varphi^{(1)}_a\rangle=E^{(1)}_a\,|\varphi^{(1)}_a\rangle\;\;,\;a=1,\ldots N_1\quad,\quad H_2|\varphi^{(2)}_b\rangle=E^{(2)}_b|\varphi^{(2)}_b\rangle\;\;,\;b=1,\ldots N_2\;. \tag{5.4}$$

Suppose that there is no interaction between the two systems. Then the energies should just add up and we should have for the Hamiltonian H acting in the tensor product space, i.e. on the combined system

$$H\ |\varphi_a^{(1)}\rangle \otimes |\varphi_b^{(2)}\rangle = (E_a^{(1)} + E_b^{(2)})|\varphi_a^{(1)}\rangle \otimes |\varphi_b^{(2)}\rangle\ , \quad \text{(no interaction)}\ . \tag{5.5}$$

But this equals

$$\begin{aligned} H\ |\varphi_a^{(1)}\rangle \otimes |\varphi_b^{(2)}\rangle &= E_a^{(1)}|\varphi_a^{(1)}\rangle) \otimes |\varphi_b^{(2)}\rangle + E_b^{(2)}|\varphi_a^{(1)}\rangle \otimes |\varphi_b^{(2)}\rangle \\ &= (H_1|\varphi_a^{(1)}\rangle) \otimes |\varphi_b^{(2)}\rangle + |\varphi_a^{(1)}\rangle \otimes (H_2|\varphi_b^{(2)}\rangle) \\ &\equiv \big(H_1 \otimes \mathbf{1} + \mathbf{1} \otimes H_2\big)|\varphi_a^{(1)}\rangle \otimes |\varphi_b^{(2)}\rangle\ . \end{aligned} \tag{5.6}$$

The last equality defines what we mean by $A \otimes \mathbf{1} + \mathbf{1} \otimes B$. It precisely means to act with A on the first factor of a factorised state and with B on the second factor of the same factorised state and then to add the two resulting vectors. This is then extended by linearity to states that are not factorised. So in general

$$\big(A \otimes \mathbf{1} + \mathbf{1} \otimes B\big) \sum_{a,b} c_{ab}\, |1:a\rangle \otimes |2:b\rangle = \sum_{a,b} c_{ab} \Big((A\,|1:a\rangle) \otimes |2:b\rangle + |1:a\rangle \otimes (B\,|2:b\rangle) \Big)\ . \tag{5.7}$$

While the correct way of writing is $A \otimes \mathbf{1} + \mathbf{1} \otimes B$, if it is clear that A acts in the first vector space and B in the second, one often simply writes $A + B$. But again, not all linear operators acting on the tensor product space are of this form. Linear operators of this form are a special subclass. For the Hamiltonian this meant that there is no interaction energy.

Very often we think of an interaction energy as resulting from the product of a certain quantity measured on the first system, multiplying some quantity measured on the second system. The corresponding operators would have the form

$$O_{A,B} = \big(A \otimes \mathbf{1}\big)\big(\mathbf{1} \otimes B\big) = A \otimes B = \big(\mathbf{1} \otimes B\big)\big(A \otimes \mathbf{1}\big)\ . \tag{5.8}$$

One may choose a basis of eigenstates $|a\rangle$ of A (with eigenvalues α_a) for the first system, and a basis of eigenstates $|b\rangle$ of B (with eigenvalues β_b) or the second system. Then $|a\rangle \otimes |b\rangle$ forms a basis of the tensor product space and evaluating any of the 3 different writings of $O_{A,B}$ on any basis state always results in

$$O_{A,B}\,|a\rangle \otimes |b\rangle = \alpha_a \beta_b\,|a\rangle \otimes |b\rangle\ \ . \tag{5.9}$$

This also proves that the three different writings of $O_{A,B}$ indeed give the same operator.[26] Again, if it is clear that A acts in the first space and B in the second, one often simply writes AB or BA instead. One sees from (5.9) that this is still a particular class of operators since there is a

[26] Of course, $\big(A \otimes \mathbf{1} + \mathbf{1} \otimes B\big)$ is *not* the same as $A \otimes B$.

basis in which the eigenvectors of this operator factorise. The most general linear operator on the tensor product space would just be defined by giving its action on all the basis vectors as

$$O\,|a\rangle \otimes |b\rangle = \sum_{c,d} |c\rangle \otimes |d\rangle\, O_{c,d|a,b}\ , \tag{5.10}$$

where the complex numbers $O_{c,d|a,b}$ are the matrix elements of O in this basis.

Since we have defined the hermitian inner product on the tensor product space, it is totally straightforward to define $O^\dagger$. In particular the matrix corresponding to $O^\dagger$ is the hermitian conjugate matrix to the one corresponding to O :

$$(O^\dagger)_{c,d|a,b} = (O_{a,b|c,d})^*\ . \tag{5.11}$$

Exercise 5.1 : *Show that if A and B or linear operators on $\mathcal{H}_{(1)}$ and $\mathcal{H}_{(2)}$ then*

$$\big(A\otimes \mathbf{1} + \mathbf{1}\otimes B\big)^\dagger = A^\dagger \otimes \mathbf{1} + \mathbf{1}\otimes B^\dagger \quad , \quad \big(A\otimes B\big)^\dagger = A^\dagger \otimes B^\dagger\ . \tag{5.12}$$

In particular, there is nothing like reversing the order between the two factors of the tensor product.

5.3 Two spin-$\frac{1}{2}$, singlet and triplet

Similarly to the way we defined the total Hamiltonian for two non-interacting systems, if we have two spin-$\frac{1}{2}$, then we can define the "total spin in the z-direction" as the eigenvalue of the operator $S_z^{\rm tot} = S_z^{(1)}\otimes \mathbf{1} + \mathbf{1}\otimes S_z^{(2)}$.

More generally, for two spin-$\frac{1}{2}$, we define for all three components of the spin operators

$$S_a^{\rm tot} = S_a^{(1)}\otimes \mathbf{1} + \mathbf{1}\otimes S_a^{(2)}\ . \tag{5.13}$$

Then with the basis states $|\pm,\pm\rangle \equiv |1:\pm\rangle\otimes|2:\pm\rangle$ we find

$$\begin{aligned}
S_z^{\rm tot}\,|{+}{+}\rangle &= \frac{\hbar}{2}\,|{+}{+}\rangle + \frac{\hbar}{2}\,|{+}{+}\rangle = \hbar\,|{+}{+}\rangle \\
S_z^{\rm tot}\,|{+}{-}\rangle &= \frac{\hbar}{2}\,|{+}{-}\rangle - \frac{\hbar}{2}\,|{+}{-}\rangle = 0 \\
S_z^{\rm tot}\,|{-}{+}\rangle &= -\frac{\hbar}{2}\,|{-}{+}\rangle + \frac{\hbar}{2}\,|{-}{+}\rangle = 0 \\
S_z^{\rm tot}\,|{-}{-}\rangle &= -\frac{\hbar}{2}\,|{-}{-}\rangle - \frac{\hbar}{2}\,|{-}\rangle = -\hbar\,|{-}{-}\rangle\ .
\end{aligned} \tag{5.14}$$

We see that the eigenvalues of the observable "total spin in the z direction" are $+\hbar, 0, -\hbar$, but with the zero eigenvalue occurring twice. One says this zero eigenvalue is two times degenerate. Hence any linear combination of the two corresponding eigenstates is still an eigenvector with this zero eigenvalue. There is a symmetric linear combination (symmetric with respect to the exchange

of the roles of the two spins) and an anti-symmetric one. Since $|{+}{+}\rangle$ and $|{-}{-}\rangle$ are also symmetric we will group the eigenstate as

$$\begin{aligned} &\text{triplet}: \qquad |{+}{+}\rangle \ , \quad \frac{1}{\sqrt{2}}\big(\,|{+}{-}\rangle + |{-}{+}\rangle\,\big) \ , \quad |{-}{-}\rangle \ , \\ &\text{singlet}: \qquad \frac{1}{\sqrt{2}}\big(\,|{+}{-}\rangle - |{-}{+}\rangle\,\big) \ . \end{aligned} \tag{5.15}$$

The 3 triplet states and the singlet state together still form a basis of the product Hilbert space, but it is no longer a basis of factorised states. In particular, the singlet state is an entangled state (as is the "middle state" of the triplet). The reason why we separated the states as triplet and singlet is the following. One can define the operators $\vec{S}^2_{\rm tot} = \sum_{j=1,2,3}(S^{\rm tot}_j)^2$. This will be discussed in more detail later on when we discuss the addition of angular momenta, but it is already a good exercise to evaluate this operator on the states. First recall that the action of the individual spin operators on the individual spin states in the z-basis was given in (3.19) as $S_x = \frac{\hbar}{2}\big(\,|{-}\rangle\langle{+}| + |{+}\rangle\langle{-}|\,\big)$, $S_y = \frac{\hbar}{2}\big(i\,|{-}\rangle\langle{+}| - i\,|{+}\rangle\langle{-}|\,\big)$ and $S_z = \frac{\hbar}{2}\big(\,|{+}\rangle\langle{+}| - |{-}\rangle\langle{-}|\,\big)$. Then

$$\begin{aligned} (S^{\rm tot}_x)^2\,|{+}{+}\rangle &= \big(S^{(1)}_x\otimes\mathbf{1} + \mathbf{1}\otimes S^{(2)}_x\big)\big(S^{(1)}_x\otimes\mathbf{1} + \mathbf{1}\otimes S^{(2)}_x\big)\,|{+}{+}\rangle \\ &= \big(S^{(1)}_x\otimes\mathbf{1} + \mathbf{1}\otimes S^{(2)}_x\big)\,\frac{\hbar}{2}\big(\,|{-}{+}\rangle + |{+}{-}\rangle\,\big) \\ &= \frac{\hbar^2}{4}\big(\,|{+}{+}\rangle + |{-}{-}\rangle + |{-}{-}\rangle + |{+}{+}\rangle\,\big) = \frac{\hbar^2}{2}\big(\,|{+}{+}\rangle + |{-}{-}\rangle\,\big) \ . \end{aligned} \tag{5.16}$$

Similarly

$$\begin{aligned} (S^{\rm tot}_y)^2\,|{+}{+}\rangle &= \big(S^{(1)}_y\otimes\mathbf{1} + \mathbf{1}\otimes S^{(2)}_y\big)\big(S^{(1)}_y\otimes\mathbf{1} + \mathbf{1}\otimes S^{(2)}_y\big)\,|{+}{+}\rangle \\ &= \big(S^{(1)}_y\otimes\mathbf{1} + \mathbf{1}\otimes S^{(2)}_y\big)\,\frac{\hbar}{2}\big(i\,|{-}{+}\rangle + i\,|{+}{-}\rangle\,\big) \\ &= \frac{\hbar^2}{4}\big((-i)i\,|{+}{+}\rangle + i^2\,|{-}{-}\rangle + i^2\,|{-}{-}\rangle + (-i)i\,|{+}{+}\rangle\,\big) = \frac{\hbar^2}{2}\big(\,|{+}{+}\rangle - |{-}{-}\rangle\,\big) \end{aligned} \tag{5.17}$$

and

$$\begin{aligned} (S^{\rm tot}_z)^2\,|{+}{+}\rangle &= \big(S^{(1)}_z\otimes\mathbf{1} + \mathbf{1}\otimes S^{(2)}_z\big)\big(S^{(1)}_z\otimes\mathbf{1} + \mathbf{1}\otimes S^{(2)}_z\big)\,|{+}{+}\rangle \\ &= \big(S^{(1)}_z\otimes\mathbf{1} + \mathbf{1}\otimes S^{(2)}_z\big)\,\hbar\,|{+}{+}\rangle \\ &= \hbar^2\,|{+}{+}\rangle) \ . \end{aligned} \tag{5.18}$$

Altogether we find

$$\vec{S}^2_{\rm tot}\,|{+}{+}\rangle = 2\hbar^2\,|{+}{+}\rangle \ . \tag{5.19}$$

Exercise 5.2 : *Compute similarly the action of $(S^{\rm tot}_x)^2$, $(S^{\rm tot}_y)^2$ and $(S^{\rm tot}_z)^2$ on the other states of the triplet and on the singlet and deduce that*

$$\begin{aligned}
\vec{S}^2_{\rm tot}\frac{1}{\sqrt{2}}\big(\,|+-\rangle+|-+\rangle\,\big) &= 2\hbar^2\,\frac{1}{\sqrt{2}}\big(\,|+-\rangle+|-+\rangle\,\big)\\
\vec{S}^2_{\rm tot}\,|--\rangle &= 2\hbar^2\,\,|--\rangle\\
\vec{S}^2_{\rm tot}\frac{1}{\sqrt{2}}\big(\,|+-\rangle-|-+\rangle\,\big) &= 0\ .
\end{aligned}\tag{5.20}$$

We see that the states of the triplet all are eigenvectors of $\vec{S}^2_{\rm tot}$ with eigenvalue $2\hbar^2$ and the singlet is also eigenvector of $\vec{S}^2_{\rm tot}$ but with eigenvalue 0. This will be interpreted later on as "all states in the triplet have spin 1 and the singlet has spin 0". With this in mind, we can also label these states now as $|S,M\rangle$ by the value $S=1$ or $S=0$ of their (total) spin and the eigenvalue M of $S^{\rm tot}_z$ (divided by $\hbar$). With this notation we can write the triplet and singlet states as

$$\begin{aligned}
&\text{triplet}: \qquad |1,1\rangle=|++\rangle\ ,\quad |1,0\rangle=\frac{1}{\sqrt{2}}\big(\,|+-\rangle+|-+\rangle\,\big)\ ,\quad |1,-1\rangle=|--\rangle\ ,\\
&\text{singlet}: \qquad |0,0\rangle=\frac{1}{\sqrt{2}}\big(\,|+-\rangle-|-+\rangle\,\big)\ .
\end{aligned}\tag{5.21}$$

These states have been written using the tensor product basis obtained by taking the (tensor) products of the individual z-basis'. To emphasise this we can rewrite e.g. the singlet state as $|0,0\rangle=\frac{1}{\sqrt{2}}\big(\,|+\rangle_z\otimes|-\rangle_z-|-\rangle_z|+\rangle_z\,\big)$ However, we could also use a tensor product basis obtained by taking the (tensor) product of other individual basis, e.g. the x-basis. Recall that $|\pm\rangle_z=\frac{1}{\sqrt{2}}\big(\,|+\rangle_x\pm|-\rangle_x\,\big)$.

Exercise 5.3 : *Show that when using the x-basis or the y-basis the singlet state becomes*

$$|0,0\rangle=\frac{1}{\sqrt{2}}\big(\,|+\rangle_x\otimes|-\rangle_x-|-\rangle_x\otimes|+\rangle_x\,\big)=\frac{1}{\sqrt{2}}\big(\,|+\rangle_y\otimes|-\rangle_y-|-\rangle_y\otimes|+\rangle_y\,\big)\ .\tag{5.22}$$

This looks very similar to the expression in the z-basis. One can similarly show that also using any individual basis of $|\pm\rangle_{\vec{u}}$ the singlet state is always looks the same. As we will see later, this is due to the fact that this state is invariant under rotations and therefore it cannot matter with respect to which direction we chose the basis states. Of course, this is *not* true for the triplet states.

5.4 Hyperfine structure

As mentioned above, we may think of the first spin-$\frac{1}{2}$ as the spin of the proton in a hydrogen atom and of the second spin-$\frac{1}{2}$ as the spin of the electron. As discussed extensively with the Stern-Gerlach experiment both particles have magnetic moments associated with their spin $\vec{m}_p=\gamma_p\vec{S}^{(1)}$ and $\vec{m}_e=\gamma_e\vec{S}^{(2)}$. Recall that $\gamma_p>0$ and $\gamma_e<0$. A magnetic dipole creates a magnetic field and this results in an interaction with the other dipole. Classically there is a dipole-dipole interaction energy

$$E_{\rm dip-dip}=-\frac{\mu_0}{4\pi}\,\frac{1}{r^3}\big(3\vec{m}_p\cdot\vec{n}\ \vec{m}_e\cdot\vec{n}-\vec{m}_p\cdot\vec{m}_e\big)\ .\tag{5.23}$$

Here $\vec{r}$ is the position vector of the electron with respect to the proton, $r = |\vec{r}|$ and $\vec{n} = \frac{\vec{r}}{r}$. One is mostly interested in studying the effect of this coupling for the (orbital) ground state of the hydrogen atom, called 1s. However, when this dipole-dipole energy is "averaged" with a spherically symmetric distribution of the position of the electron (which is the case for the 1s spatial probability distribution) this vanishes.[27] Instead, a more thorough discussion shows that there is still a similar term which involves the modulus square of the ground state wave function at the origin (at the position of the proton) and the scalar product of the two magnetic moments. Without going into details, let us take as Hamiltonian

$$H_{\rm hf} = -\kappa \, \frac{\mu_0}{4\pi r_0^3} \, \vec{m}_p \cdot \vec{m}_e = -\kappa \, \frac{\mu_0 \gamma_e \gamma_p}{4\pi r_0^3} \, \vec{S}^{(1)} \cdot \vec{S}^{(2)} = \kappa \, \frac{\mu_0 |\gamma_e \gamma_p|}{4\pi r_0^3} \, \vec{S}^{(1)} \cdot \vec{S}^{(2)} \ , \tag{5.24}$$

where κ is some number of order one and r_0 is a characteristic length scale which we take to be the Bohr radius. What do we mean by the operator $\vec{S}^{(1)} \cdot \vec{S}^{(2)}$? This was discussed above for the interaction between two systems. This expression is just short-hand for

$$\vec{S}^{(1)} \cdot \vec{S}^{(2)} = \sum_{a=x,y,z} S_a^{(1)} \otimes S_a^{(2)} \ . \tag{5.25}$$

On the other hand, from our rule (5.8) for multiplying operators on the tensor product space and our definition (5.13) of the total spin it follows that

$$\begin{aligned} S_a^{\rm tot} S_b^{\rm tot} &= \big(S_a^{(1)} \otimes \mathbf{1} + \mathbf{1} \otimes S_a^{(2)}\big)\big(S_b^{(1)} \otimes \mathbf{1} + \mathbf{1} \otimes S_b^{(2)}\big) \\ &= S_a^{(1)} S_b^{(1)} \otimes \mathbf{1} + \mathbf{1} \otimes S_a^{(2)} S_b^{(2)} + S_a^{(1)} \otimes S_b^{(2)} + S_b^{(1)} \otimes S_a^{(2)} \ . \end{aligned} \tag{5.26}$$

If we now set $a = b$ and sum over $a = x, y, z$ we get

$$\vec{S}_{\rm tot}^2 = \vec{S}_{(1)}^2 \otimes \mathbf{1} + \mathbf{1} \otimes \vec{S}_{(2)}^2 + 2 \sum_{a=x,y,z} S_a^{(1)} \otimes S_a^{(2)} \tag{5.27}$$

Now, $\vec{S}_{(1)}^2 \, |\pm\rangle = \frac{3}{4}\hbar^2 \, |\pm\rangle$ and $\vec{S}_{(2)}^2 \, |\pm\rangle = \frac{3}{4}\hbar^2 \, |\pm\rangle$ so that within our tensor product Hilbert space, we may rewrite (5.27) as

$$\vec{S}^{(1)} \cdot \vec{S}^{(2)} = \frac{1}{2} \vec{S}_{\rm tot}^2 - \frac{3}{4}\hbar^2 \, \mathbf{1} \otimes \mathbf{1} \ . \tag{5.28}$$

We see that the eigenvectors of this operator are precisely the 3 triplet states with eigenvalue $+\frac{\hbar^2}{4}$ and the singlet with eigenvalue $-\frac{3}{4}\hbar^2$. For the hyperfine Hamiltonian (5.24) this then yields

$$H_{\rm hf} \, |1, M\rangle = \frac{1}{4} \, \frac{\kappa \, \mu_0 \hbar^2 |\gamma_e \gamma_p|}{4\pi r_0^3} \, |1, M\rangle \ , \quad M = -1, 0, 1 \quad , \quad H_{\rm hf} \, |0, 0\rangle = -\frac{3}{4} \, \frac{\kappa \, \mu_0 \hbar^2 |\gamma_e \gamma_p|}{4\pi r_0^3} \, |0, M\rangle \ . \tag{5.29}$$

[27] This is easy to see in the simple example where both $\vec{m}_e$ and $\vec{m}_p$ are aligned. If we call θ the angle between these dipole moments and the position vector $\vec{r}$, then the expression in the bracket is $|\vec{m}_e| \, |\vec{m}_p| (3\cos^2\theta - 1)$. Averaging with a spherically symmetric distribution means integrating with $\frac{1}{4\pi} \int_0^{2\pi} {\rm d}\varphi \int_0^{\pi} {\rm d}\theta \, \sin\theta$ and (changing variables as $x = \cos\theta$) one sees that $\int_0^{\pi} {\rm d}\theta \, \sin\theta (3\cos^2\theta - 1) = \int_{-1}^{1} {\rm d}x (3x^2 - 1) = 0$.

It turns out that the numerical constant is $\kappa = \frac{8}{3}$ and then the difference of these eigenvalues (the hyperfine splitting) is

$$\Delta E_{\rm hf} = \frac{8}{3}\frac{\mu_0 \hbar^2 |\gamma_e \gamma_p|}{4\pi r_0^3} \ . \tag{5.30}$$

Numerical estimates : Let us estimate this quantity. In general, when trying to numerically estimate atomic quantities it is useful to deal with as few dimensionful quantities as possible. It is then useful to introduce the so-called fine-structure constant α given by

$$\alpha = \frac{q^2}{4\pi\epsilon_0 \hbar c} \simeq \frac{1}{137} \ , \tag{5.31}$$

where q is the elementary charge, i.e the charge of the proton (or the opposite of the charge of the electron). Furthermore

$$\mu_0 = \frac{1}{\epsilon_0 c^2} \ . \tag{5.32}$$

Next recall $|\gamma_e| = g_e \frac{q}{2m_e}$ and $\gamma_p = g_p \frac{q}{2m_p}$ where $g_e \simeq 2$ and $g_p \simeq 5.6$. Then already

$$\Delta E_{\rm hf} = \frac{8}{3}\frac{g_e g_p \alpha c^2}{4 m_e m_p}\Big(\frac{\hbar}{c r_0}\Big)^3 \ . \tag{5.33}$$

We will take for r_0 the Bohr radius[28] $r_0 = \frac{\hbar}{m_e c \alpha}$ so that $\frac{\hbar}{c r_0} = m_e \alpha$ and

$$\Delta E_{\rm hf} = \frac{8}{3}\frac{g_e g_p}{2}\frac{m_e}{m_p}\frac{m_e c^2 \alpha^2}{2}\,\alpha^2 \ . \tag{5.34}$$

Now, $\frac{g_e g_p}{2} \simeq 5.6$, $\frac{m_e}{m_p} \simeq \frac{1}{1836}$ and $\frac{m_e c^2 \alpha^2}{2} \simeq 13.6$ eV. One ends up with

$$\Delta E_{\rm hf} \simeq 5.9 \times 10^{-6}\,{\rm eV} \ . \tag{5.35}$$

Planck's constant was given in (1.6) as $h \simeq 4.1\ 10^{-15}\,{\rm eV\,s}$, so that this corresponds to a frequency of $\nu_{\rm hf} = \frac{\Delta E_{\rm hf}}{h} \simeq 1.4$ GHz, and to a wavelength of $\lambda = \frac{c}{\nu} \simeq 21\,{\rm cm}$, indeed !

5.5 Measuring observables of one of the two systems

Suppose we have some state in the Hilbert space of two spin-$\frac{1}{2}$. This can be an arbitrary linear superposition of the 4 basis states. Since the two spins are distinguishable we can decide to measure the z-component of the first spin. If we find $+\frac{\hbar}{2}$ then the state of the first spin will be $|1:+\rangle$ after the measurement, and similarly if we find $-\frac{\hbar}{2}$ the state of the first spin will be

[28] A nice way to recover the Bohr radius (and ground state energy of the hydrogen atom) is to write the classical energy $E = \frac{\vec{p}^{\,2}}{2m_e} - \frac{q^2}{4\pi\epsilon_0 r}$, replace $\vec{p}^{\,2}$ by an estimate from the uncertainty relation as $\vec{p}^{\,2} \to \frac{\hbar^2}{r^2}$ and minimise the energy function obtained, $E(r) = \frac{\hbar^2}{2m_e r^2} - \frac{q^2}{4\pi\epsilon_0 r}$ with respect to r. This is minimum at $r = r_0 = \frac{4\pi\epsilon_0\hbar^2}{m_e q^2} = \frac{\hbar}{m_e c\alpha}$ which is the Bohr radius. Moreover, $E(r_0) = -\frac{1}{2}m_e c^2\alpha^2$ is the exact ground state energy of -13.6 eV ! In general such semi-classical arguments give a good order of magnitude estimate. It is fortunate that here we actually get the exact results.

$|1:-\rangle$. This "reduction of the wave packet" will be done by applying the corresponding projector $P(1:\pm) = |1:\pm\rangle\langle 1:\pm| \otimes \mathbf{1} \equiv |+\rangle\langle +| \otimes \mathbf{1}$.

Let's suppose the two spin-$\frac{1}{2}$ system is in the singlet state, e.g. because this is the ground state from the hyperfine splitting, or for any other reason : $|\psi\rangle = |0,0\rangle = \frac{1}{\sqrt{2}}\big(|+-\rangle - |-+\rangle\big)$. And suppose the measurement of the z-component of the first spin gives $+\frac{\hbar}{2}$. Then applying $P(1:+)$ on this state gives

$$P(1:+)\,|\psi\rangle = \big(|+\rangle\langle +| \otimes \mathbf{1}\big)\ \frac{1}{\sqrt{2}}\big(|+-\rangle - |-+\rangle\big) = \frac{1}{\sqrt{2}}\,|+-\rangle\ . \tag{5.36}$$

Upon normalising to 1, we see that the state of the combined system after the measurement is $|+-\rangle$. But this means that if one now measures the z-component of the second spin one finds $-\frac{\hbar}{2}$ with probability one. The measurement of the first spin has not only "reduced" the state of the first spin but also "reduced" the state of the second spin. This is of course, because to begin with, there was nothing like "the state of the first spin". There was only a certain state of the combined system which was the singlet state.

More generally, what is the probability to find a certain eigenvalue a_n of an observable pertaining to the first particle ? For a single particle this was given in (2.53) in terms of the projector (2.52) on the eigenspace of the eigenvalue a_n. Since at present we do not measure anything on the second system the relevant projector is

$$P_{(1)}(a_n) = \Big(\sum_{i=1}^{d_n} |\phi_n^i\rangle\langle\phi_n^i|\Big) \otimes \mathbf{1}\ , \tag{5.37}$$

where, as before, the $|\phi_n^i\rangle$ are the eigenstates of A with eigenvalue a_n. If $\{|b\rangle\}$ denotes an orthonormal basis for the second system, we may also rewrite the projector as

$$P_{(1)}(a_n) = \Big(\sum_{i=1}^{d_n} |\phi_n^i\rangle\langle\phi_n^i|\Big) \otimes \Big(\sum_b |b\rangle\langle b|\Big) = \sum_{i=1}^{d_n}\sum_b |\phi_n^i\rangle \otimes |b\rangle\ \ \langle\phi_n^i| \otimes \langle b|\ . \tag{5.38}$$

Then, if the combined system is in the state $|\Psi\rangle$, the probability to find a_n when measuring A on the first system is given, as in (2.53), by

$$\mathcal{P}_{(1)}(a_n, \Psi) = \langle\Psi|\, P_{(1)}(a_n)\,|\Psi\rangle\ . \tag{5.39}$$

All this transposes in an obvious way to computing probabilities for the second system.

Let us apply this rule to the measurement of the z-component of the first spin, if the combined state is a singlet, i.e. $|\Psi\rangle = |0,0\rangle$, we find

$$\begin{aligned}
\mathcal{P}_{(1)}\big(\frac{\hbar}{2}, \text{singlet}\big) &= \langle 0,0|\,\Big(|+\rangle\langle +| \otimes \mathbf{1}\Big)\,|0,0\rangle \\
&= \frac{1}{\sqrt{2}}\Big(\langle +-| - \langle -+|\Big)\Big(|+\rangle\langle +| \otimes \mathbf{1}\Big)\ \frac{1}{\sqrt{2}}\Big(|+-\rangle - |-+\rangle\Big) \\
&= \frac{1}{2}\langle +-|+-\rangle = \frac{1}{2}\ ,
\end{aligned} \tag{5.40}$$

as expected. Of course, one also finds similarly that $\mathcal{P}_{(1)}\big(-\frac{\hbar}{2}, \text{singlet}\big) = \frac{1}{2}$. We may also ask "what is the probability that a measurement of the z-component of the first spin gives $\frac{\hbar}{2}$ and a measurement of the z-component of the second spin gives $-\frac{\hbar}{2}$?" Obviously, this is $\frac{1}{2} \times 1 = \frac{1}{2}$. Obviously also, the probability that both measurements give $+\frac{\hbar}{2}$ vanishes, etc.

Maybe more interestng is the following question : "what is the probability that a measurement of the z-component of the first spin gives $\frac{\hbar}{2}$ and a measurement of the x-component of the second spin gives $-\frac{\hbar}{2}$?" Because of the "reduction of the wave packet" by the first measurement, let us be precise and decide that the measurement on the first spin is done first and the measurement on the second spin only an instant later. We have seen that the first measurement finds $\frac{\hbar}{2}$ with probability $\frac{1}{2}$ and that after this measurement the state is $|+-\rangle \equiv |+\rangle_z \otimes |-\rangle_z$. The probability that the subsequent measurement of the x-component of the spin of the second particle gives $-\frac{\hbar}{2}$ is

$$\langle +|_z \otimes \langle -|_z \Big(\mathbf{1} \otimes |-\rangle_x \langle -|_x \Big) |+\rangle_z \otimes |-\rangle_z = \langle +|_z |+\rangle_z \langle -|_z |-\rangle_x \langle -|_x |-\rangle_z = 1 \times \frac{1}{\sqrt{2}} \times \frac{1}{\sqrt{2}} = \frac{1}{2} \ . \tag{5.41}$$

Thus the joint probability to find first $\frac{\hbar}{2}$ when measuring the z-component of the first spin and then find $-\frac{\hbar}{2}$ when measuring the x-component of the second spin is $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$. Let us now reverse the order of the two measurements. Since the singlet state can be written equivalently as in (5.22) it is very easy to see that one again finds a joint probability $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$.

Let us now repeat the two measurements but for a state that is $|++\rangle \equiv |+\rangle_z \otimes |+\rangle_z$. Then the first measurement of the z-component will give $\frac{\hbar}{2}$ with probability 1 and the state remains the same after the measurement, and then measuring $-\frac{\hbar}{2}$ on the x-component of the second spin will occur with a probability

$$\langle +|_z \otimes \langle +|_z \Big(\mathbf{1} \otimes |-\rangle_x \langle -|_x \Big) |+\rangle_z \otimes |+\rangle_z = \langle +|_z |+\rangle_z \langle +|_z |-\rangle_x \langle -|_x |+\rangle_z = \frac{1}{2} \ , \tag{5.42}$$

and the state will be, after the measurement $|+\rangle_z \otimes |-\rangle_x$. What if we do the measurements in the opposite order on this $|++\rangle \equiv |+\rangle_z \otimes |+\rangle_z$ state? If we first measure the x-component of the second spin we will find $-\frac{\hbar}{2}$ with probability $\frac{1}{2}$ and then the state is $|+\rangle_z \otimes |-\rangle_x$ after this measurement. Measuring then the z component of the first spin gives $\frac{\hbar}{2}$ with probability 1. Overall, we find the same results and the same probabilities for both order of measurements.

More generally, suppose we have an observable A defined for the first system and an observable B defined on the second system. What is the probability that a measurement of A on the first system yields a_n and then a measurement of B on the second system yields b_m ? To simplify the discussion, suppose that the eigenvalues of A and B are non degenerate. Then a basis of the tensor product space is given by the tensor products of the eigenbasis' of these A and B, namely $|a_n\rangle \otimes |b_m\rangle$ and a general state is

$$|\psi\rangle = \sum_{k,l} c_{kl} \, |a_k\rangle \otimes |b_l\rangle \quad , \quad \text{with} \quad \sum_{k,l} |c_{kl}|^2 = 1 \ . \tag{5.43}$$

The probability that a first measurement of A on the first system yields a_n is

$$\mathcal{P}_{(1)}(a_n,\psi) = \langle\psi|\, P(a_n)\otimes \mathbf{1}\,|\psi\rangle = \sum_l |c_{nl}|^2 \ , \tag{5.44}$$

and the state after the measurement is

$$|\psi'\rangle = \frac{P(a_n)\otimes \mathbf{1}\,|\psi\rangle}{||P(a_n)\otimes \mathbf{1}\,|\psi\rangle\,||} = \frac{\sum_l c_{nl}\,|a_n\rangle\otimes|b_l\rangle}{\sqrt{\sum_l |c_{nl}|^2}} \ . \tag{5.45}$$

The probability that a subsequent measurement of B yields b_m then is

$$\mathcal{P}_{(2)}(b_m,\psi') = \langle\psi'|\, \mathbf{1}\otimes P(b_m)\,|\psi'\rangle = \frac{|c_{nm}|^2}{\sum_l |c_{nl}|^2} \ , \tag{5.46}$$

and the state after this second measurement is

$$|\psi''\rangle = |a_n\rangle\otimes|b_m\rangle \ . \tag{5.47}$$

Then, the probability to measure first a_n (for A on the first system) and then b_m (for B on the second system) is

$$\mathcal{P}(a_n,b_m,\psi) = \mathcal{P}_{(1)}(a_n,\psi)\ \mathcal{P}_{(2)}(b_m,\psi') = |c_{nm}|^2 \ , \tag{5.48}$$

and the state after these two measurements is given by (5.47). We see that neither (5.48), nor (5.47) depends on the fact that we measured A first and then B. The result is totally symmetric and would have been the same if we had done the measurements in the reverse order. We conclude in general :

- The joint probabilitiy to find a_n when mesuring A on the first subsystem and b_n when measuring B on the second subsystem is independent of the order of the measurements. Also, the final state after the measurements is the same in both cases.

5.6 EPR paradox

Let us discuss further the measurements of the two spins of the singlet state. Experimentally, photons are easier to manipulate than spins. As discussed in the beginning, the polarisation of photons can be decomposed on a basis of two orthonormal basis vectors in the plane perpendicular to its momentum. We fix such a basis and denote the corresponding states as $|+\rangle$ and $|-\rangle$ and call them horizontal and vertical polarisations. They correspond to the z-basis for the spins. One can consider the linear combinations $\frac{1}{\sqrt{2}}\big(\,|+\rangle \pm |-\rangle\,\big)$. They describe polarisations at 45^o and correspond to the x-basis for the spins. Finally taking the complex linear combinations $\frac{1}{\sqrt{2}}\big(\,|+\rangle \pm i\,|-\rangle\,\big)$ describe circular polarisations and they correspond to the y-basis. A pair of photons in the singlet state can then be produced experimentally by a successive emission of two photons in an atomic transition from an excited level to an intermediate level and then to the

ground state. One can then spatially separate the two photons and to perform measurements on one or the other at (relatively) large spatial separation. But let's continue with our more familiar discussion in terms of spin-$\frac{1}{2}$.

Having produced a singlet state, one separates the two spins. A first observer, traditionally called Alice can do measurements on the first spin and another observer, called Bob, can do measurements on the second spin. We have seen that if Alice measures the spin in the z-direction and finds $\frac{\hbar}{2}$ it must be that Bob's measurement, also in the z-direction yields $-\frac{\hbar}{2}$, and vice versa. Thus, once Alice has measured her spin, she can predict with probability one what must be the outcome of Bob's measurement, provided it is along the same direction. The quantum mechanical interpretation is that there is no way of knowing in advance what Alice's measurement will yield, but once she has measured, there is the reduction of the wave packet and then she can predict the outcome of Bob's measurement. This is maybe not so surprising. Consider a classical experiment where one has a red and black card, puts each one in a separate closed envelope, shuffles the envelopes and then gives one to Alice and one to Bob. None of them knows which card is in their envelopes, but when Alice opens her envelope and discovers that her card is red, she knows for sure that Bob will find a black card in his envelope. The difference with the quantum mechanical measurement is that although neither Alice nor Bob had an a priori knowledge of their colours, nobody will doubt that the colour was determined prior to observing it and, in principle, if one had carefully observed the shuffling of the envelopes one could have known which was the colour of Alice's card. The quantum mechanical description - and interpretation - is radically different : there is no a priori determination of which result Alice will obtain. Said differently, there is no extra parameter attached to her spin which could allow some superior intelligence to know the outcome of her measurement in advance.

In a famous paper, Einstein, Podolsky and Rosen (EPR) have argued in 1935 that the quantum mechanical description couldn't be the ultimate description but that there should be some hidden parameter (or hidden variable) which if known would allow an a priori determination of the outcome of the measurements: "God does not play dice". It did not seem conceivable to them that a measurement done by Alice could predict instantaneously the outcome of Bob's measurement, in particular if Bob is far away, unless both outcomes are determined in advance by such a hidden variable. Of course, EPR did not try to invalidate the quantum mechanical formalism which already had proven extremely successful. But they argued that such a (or several) hidden variables must be present so as to reproduce all quantum mechanical formulae but providing a different and actually deterministic interpretation.

5.7 Bell's inequalities

Whether or not such hidden variables do exist or not remained purely at the level of a philosophical debate, unless one can show that one or the other interpretation leads to different experimentally verifiable predictions. It was the discovery by Bell almost 30 years later, in 1964, that one could indeed distinguish between the existence or non-existence of hidden variables. He showed very generally that if the outcome of the experiments is dictated by some set of hidden (local) variables in a deterministic way, then certain observable quantities must satisfy a certain bound. These are Bell's inequalities. If the experiment shows that this bound is violated there cannot be any hidden (local) variables. In the 1970' and early 80' various experimental groups have attempted to measure these quantities. The conclusive result was obtained by the Orsay group led by Aspect who obtained a value of 2.7 where Bell's inequality set a bound of 2. This settled the debate and fundamentally established the quantum mechanical indeterminism. The Nobel Prize in Physics 2022 was awarded to Alain Aspect, John F. Clauser and Anton Zeilinger "for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science".

Let us now establish Bell's inequalities. It involves measuring the spin along different directions given by unit vectors $\vec{u}_a$ and $\vec{u}_a^{'}$ for Alice (the first spin) and $\vec{u}_b$ and $\vec{u}_b^{'}$ for Bob (second spin). Let us introduce the correlation function $E(\vec{u}_a, \vec{u}_b)$ which is the mean value of the product of Alice's spin measurements in the $\vec{u}_a$ direction and of Bob's spin measurements in the $\vec{u}_b$ direction, divided by $\frac{\hbar^2}{4}$. It's value is always comprised between -1 (perfect anti-correlation of the spins) and $+1$ (perfect correlation). In particular, from our discussion above, we know that we should find $E(\vec{u}_a, \vec{u}_a) = -1$ or $E(\vec{u}_a, -\vec{u}_a) = 1$ which just states that if Alice measures along an axis and finds $\pm\frac{\hbar}{2}$ then along the same axis Bob finds $\mp\frac{\hbar}{2}$ or along the opposite axis he finds $\pm\frac{\hbar}{2}$. More generally for different directions $\vec{u}_a$ and $\vec{u}_b$ each individual measurement either gives the product $+\frac{\hbar^2}{4}$ or $-\frac{\hbar^2}{4}$, and then the average for many measurements must be between $-\frac{\hbar^2}{4}$ and $+\frac{\hbar^2}{4}$, so that indeed,

$$|E(\vec{u}_a, \vec{u}_b)| \leq 1 \ . \tag{5.49}$$

What could be said about this quantity $E(\vec{u}_a, \vec{u}_b)$ in a theory of hidden variables ? A hidden variable consists of a parameter, or possibly multiple parameters, which we denote λ and which can take values in some set Λ. There must then exist some well-defined function $A(\lambda, \vec{u}_a)$ that determines for every direction $\vec{u}_a$ of measurement of the spin by Alice whether the result is $+\frac{\hbar}{2}$ or $-\frac{\hbar}{2}$, i.e. $A(\lambda, \vec{u}_a) = \pm\frac{\hbar}{2}$. More precisely, there is a subset $\Lambda_+(\vec{u}_a)$ such that for $\lambda \in \Lambda_+(\vec{u}_a)$ we have $A(\lambda, \vec{u}_a) = +\frac{\hbar}{2}$ and for $\lambda \in \Lambda_-(\vec{u}_a) = \Lambda - \Lambda_+(\vec{u}_a)$ we have $A(\lambda, \vec{u}_a) = -\frac{\hbar}{2}$. There is a certain locality assumption here since we suppose that this function for Alice does not depend on the direction $\vec{u}_b$ used by Bob. There is similarly a function $B(\lambda, \vec{u}_b)$ determining the outcome of Bob's measurement of the second spin in the $\vec{u}_b$ direction. Let $\mathcal{P}(\lambda)$ be the distribution of λ which can be very general. It would be known by some superior intelligence but not to us. However it must

be non-negative and normalised :

$$\mathcal{P}(\lambda) \geq 0 \quad , \quad \int_\Lambda \mathrm{d}\lambda\, \mathcal{P}(\lambda) = 1 \ , \tag{5.50}$$

where $\mathrm{d}\lambda$ possibly stands for some multi-dimensional volume element on Λ. Then the function $E(\vec{u}_a, \vec{u}_b)$ is given by

$$E_{\text{hidden}}(\vec{u}_a, \vec{u}_b) = \frac{4}{\hbar^2} \int_\Lambda \mathrm{d}\lambda\, \mathcal{P}(\lambda)\, A(\lambda, \vec{u}_a)\, B(\lambda, \vec{u}_b) \ . \tag{5.51}$$

On the other hand, in quantum mechanics, if the quantum state is the singlet $|0,0\rangle$, this function is given by

$$E_{\text{QM}}(\vec{u}_a, \vec{u}_b) = \frac{4}{\hbar^2} \langle 0,0|\, \vec{u}_a \cdot \vec{S} \otimes \vec{u}_b \cdot \vec{S}\, |0,0\rangle \ . \tag{5.52}$$

We have seen before that we could write the singlet state in the same form using the eigenbasis $|\pm\rangle_{\vec{u}}$ of $\vec{S} \cdot \vec{u}$ for any unit vector $\vec{u}$. We choose the eigenbasis $|\pm\rangle_{\vec{u}_a}$ with $\vec{u}_a \cdot \vec{S}\, |\pm\rangle_{\vec{u}_a} = \pm\frac{\hbar}{2}\, |\pm\rangle_{\vec{u}_a}$ and

$$|0,0\rangle = \frac{1}{\sqrt{2}} \big(|+\rangle_{\vec{u}_a} \otimes |-\rangle_{\vec{u}_a} - |-\rangle_{\vec{u}_a} \otimes |+\rangle_{\vec{u}_a} \big) \ . \tag{5.53}$$

Then

$$\frac{2}{\hbar} \vec{u}_a \cdot \vec{S} \otimes \vec{u}_b \cdot \vec{S} \big(|+\rangle_{\vec{u}_a} \otimes |-\rangle_{\vec{u}_a} - |-\rangle_{\vec{u}_a} \otimes |+\rangle_{\vec{u}_a} \big) = |+\rangle_{\vec{u}_a} \otimes \vec{u}_b \cdot \vec{S}\, |-\rangle_{\vec{u}_a} + |-\rangle_{\vec{u}_a} \otimes \vec{u}_b \cdot \vec{S}\, |+\rangle_{\vec{u}_a} \ . \tag{5.54}$$

Upon taking the inner product with $\langle 0,0| = \frac{1}{\sqrt{2}} \big(\langle +|_{\vec{u}_a} \otimes \langle -|_{\vec{u}_a} - \langle -|_{\vec{u}_a} \otimes \langle +|_{\vec{u}_a} \big)$ one gets

$$\frac{4}{\hbar^2} \langle 0,0|\, \vec{u}_a \cdot \vec{S} \otimes \vec{u}_b \cdot \vec{S}\, |0,0\rangle = \frac{2}{\hbar}\, \frac{1}{2} \big(\langle -|_{\vec{u}_a}\, \vec{u}_b \cdot \vec{S}\, |-\rangle_{\vec{u}_a} - \langle +|_{\vec{u}_a}\, \vec{u}_b \cdot \vec{S}\, |+\rangle_{\vec{u}_a} \big) \tag{5.55}$$

One can compute this explicitly using (3.29) and (3.32) and a few trigonometric relations to find that (5.55) only depends on the angle between $\vec{u}_a$ and $\vec{u}_b$, i.e. on $\cos\theta = \vec{u}_a \cdot \vec{u}_b$. But then we may just as well compute this expression with $\vec{u}_a \to \vec{e}_z$ and $\vec{u}_b \to \vec{u}$ where $\vec{u}$ makes an angle θ with the z-axis. One sees from (3.29) that $\langle \pm|\, \vec{u} \cdot \vec{S}\, |\pm\rangle = \pm\frac{\hbar}{2} \cos\theta$ and then (5.55) equals $-\cos\theta = -\vec{u}_a \cdot \vec{u}_b$ and

$$E_{\text{QM}}(\vec{u}_a, \vec{u}_b) = -\vec{u}_a \cdot \vec{u}_b \ . \tag{5.56}$$

Now consider the quantity

$$\mathcal{S} = E(\vec{u}_a, \vec{u}_b) + E(\vec{u}_a, \vec{u}_b^{\,\prime}) - \big(E(\vec{u}_a^{\,\prime}, \vec{u}_b) - E(\vec{u}_a^{\,\prime}, \vec{u}_b^{\,\prime}) \big) \ . \tag{5.57}$$

In the hidden variable theory this equals

$$\mathcal{S}_{\text{hidden}} = \frac{4}{\hbar^2} \int_\Lambda \mathrm{d}\lambda\, \mathcal{P}(\lambda) s(\lambda) \ , \tag{5.58}$$

where

$$s(\lambda) = A(\lambda, \vec{u}_a) \Big(B(\lambda, \vec{u}_b) + B(\lambda, \vec{u}_b^{\,\prime}) \Big) - A(\lambda, \vec{u}_a^{\,\prime}) \Big(B(\lambda, \vec{u}_b) - B(\lambda, \vec{u}_b^{\,\prime}) \Big) \ . \tag{5.59}$$

Now, the $B(\lambda, \vec{u}_b)$ and $B(\lambda, \vec{u}_b^{'})$ can only take the values $\pm\frac{\hbar}{2}$ and they are either equal or opposite. In any case, one of the two brackets in the last line vanishes, and the other term then equals $\pm\frac{\hbar}{2}(\pm\hbar)$ so this is $\pm\frac{\hbar^2}{2}$. It follows that $\left| \int_\Lambda \mathrm{d}\lambda\, \mathcal{P}(\lambda) s(\lambda) \right| \leq \frac{\hbar^2}{2} \int_\Lambda \mathrm{d}\lambda\, \mathcal{P}(\lambda) = \frac{\hbar^2}{2}$ and

$$|S_{\text{hidden}}| \leq 2 \ . \tag{5.60}$$

This is Bell's inequality for any (local) hidden variable theory.

In quantum mechanics, we have

$$S_{\text{QM}} = -\vec{u}_a \cdot \vec{u}_b - \vec{u}_a \cdot \vec{u}_b^{'} + \vec{u}_a^{'} \cdot \vec{u}_b - \vec{u}_a^{'} \cdot \vec{u}_b^{'} \ . \tag{5.61}$$

By arranging the 4 unit vectors to lie in the same plane, always with a 45^o ange between two successive vectors, in this order $\vec{u}_a^{'},\ \vec{u}_b^{'},\ \vec{u}_a,\ \vec{u}_b$, one has

$$\vec{u}_a \cdot \vec{u}_b = \vec{u}_a \cdot \vec{u}_b^{'} = -\vec{u}_a^{'} \cdot \vec{u}_b = \vec{u}_a^{'} \cdot \vec{u}_b^{'} = \frac{1}{\sqrt{2}} \ , \tag{5.62}$$

so that

$$S_{\text{QM}} = -2\sqrt{2} \ , \tag{5.63}$$

obviously violating Bell's inequality. As already mentioned, the experimental results showed a clear violation of Bell's inequality and a result in agreement with the quantum mechanical prediction.

5.8 No-cloning theorem and quantum teleportation

No-cloning theorem : Let us now show a fundamental property of quantum mechanics, that it is impossible to copy (duplicate or clone) a given general state. What does copying mean ? When copying a paper e.g., starting from the original and a blanc paper one wants to get a copy but also get back the original, i.e. the blanc paper has been evolved to the copy. In quantum mechanics this means that one starts with a tensor product of the two systems, consisting of the two sheets of paper. The original is in state ψ_1 and the blanc paper in some (known) state ϕ. Then during the copying process they should evolve as

$$|1:\psi_1\rangle \otimes |2:\phi\rangle \to |1:\psi_1\rangle \otimes |2:\psi_1\rangle \ . \tag{5.64}$$

For some other (orthogonal) initial state one should have

$$|1:\psi_2\rangle \otimes |2:\phi\rangle \to |1:\psi_2\rangle \otimes |2:\psi_2\rangle \ . \tag{5.65}$$

Both copying processes must be governed by some (complicated) hermitian Hamiltonian and corresponding *linear* evolution operator. Let us now try to copy the state $|1:\psi_3\rangle = \frac{1}{\sqrt{2}}\big(\,|1:\psi_1\rangle + |1:\psi_2\rangle\,\big)$. By linearity one then has

$$\begin{aligned} |1:\psi_3\rangle \otimes |2:\phi\rangle \quad &= \quad \frac{1}{\sqrt{2}}\big(\,|1:\psi_1\rangle \otimes |2:\phi\rangle + \frac{1}{\sqrt{2}}\big(\,|1:\psi_2\rangle \otimes |2:\phi\rangle \\ &\to \quad \frac{1}{\sqrt{2}}\,|1:\psi_1\rangle \otimes |2:\psi_1\rangle + \frac{1}{\sqrt{2}}\,|2:\psi_2\rangle \otimes |2:\psi_2\rangle \ . \end{aligned} \tag{5.66}$$

This is *not* the desired result which would be

$$\rightarrow \frac{1}{\sqrt{2}}\big(\,|1:\psi_1\rangle + |1:\psi_2\rangle\,\big) \otimes \frac{1}{\sqrt{2}}\big(\,|1:\psi_1\rangle + |1:\psi_2\rangle\,\big)\ . \tag{5.67}$$

We see that the linearity of the evolution (of the Schrödinger equation) has produced the entangled state (5.66), rather than the desired factorised copy (5.67). This impossibility to duplicate (clone) an arbitrary quantum state goes under the name of "No-cloning theorem". As we will see below, it is at the basis of quantum cryptography.

Quantum teleportation protocol : Before turning to cryptography, let us discuss another particularity of quantum mechanics called quantum teleportation. The goal here is that Alice has a certain arbitrary spin-$\frac{1}{2}$ state (q-bit) and she wants to transmit the exact information about this state to her friend Bob in such a way that the information cannot be intercepted. This is done in such a way that in the end Bob has a spin-$\frac{1}{2}$ state which is exactly Alice's initial state. Of course, then Alice no longer can have her initial state since otherwise they would have managed to duplicate it - which is not possible as we have jus seen.

The protocol goes back to Bennett et al in 1993. It involves 3 q-bits, or say 3 particles of spin $\frac{1}{2}$. We call these particles A, B and C. We will then have to deal with triple tensor products and we will indicate the particles concerned by subscripts, so that $|+\rangle_A$ refers to a state of particle A, and $|+-\rangle_{BC}$ to a state of particles B and C in the corresponding tensor product space and, of course $|++-\rangle_{ABC} = |+\rangle_A \otimes |+-\rangle_{BC}$ to the state of the 3 particles in the triple tensor product space. We may suppose that the $\pm$ refer to the z-basis, but it does actually not matter which basis one uses, as long as one agrees on one direction with respect to which the individual eigenstates $|\pm\rangle$ are defined. An important role is played by a particular basis in the tensor product space of two particles, called a "Bell basis" and consisting of 4 orthogonal entangled "Bell states". They are usually denoted as $|\Phi^{\pm}\rangle$ and $|\Psi^{\pm}\rangle$ and are given by

$$\begin{aligned} \big|\Phi^+\big\rangle &= \frac{1}{\sqrt{2}}\big(\,|{+}{+}\rangle + |{-}{-}\rangle\,\big) \qquad , \qquad \big|\Phi^-\big\rangle = \frac{1}{\sqrt{2}}\big(\,|{+}{+}\rangle - |{-}{-}\rangle\,\big)\ , \\ \big|\Psi^+\big\rangle &= \frac{1}{\sqrt{2}}\big(\,|{+}{-}\rangle + |{-}{+}\rangle\,\big) \qquad , \qquad \big|\Psi^-\big\rangle = \frac{1}{\sqrt{2}}\big(\,|{+}{-}\rangle - |{-}{+}\rangle\,\big)\ . \end{aligned} \tag{5.68}$$

This is obviously a basis for the two-particle Hilbert space. (In terms of the triplet and singlet states we have $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\big(\,|1,1\rangle \pm |1,-1\rangle\,\big)$, $|\Psi^+\rangle = |1,0\rangle$ and $|\Psi^-\rangle = |0,0\rangle$.) One could retrieve the non-entangled states as

$$\begin{aligned} |{+}{+}\rangle &= \frac{1}{\sqrt{2}}\big(\,\big|\Phi^+\big\rangle + \big|\Phi^-\big\rangle\,\big) \qquad , \qquad |{-}{-}\rangle = \frac{1}{\sqrt{2}}\big(\,\big|\Phi^+\big\rangle - \big|\Phi^-\big\rangle\,\big)\ , \\ |{+}{-}\rangle &= \frac{1}{\sqrt{2}}\big(\,\big|\Psi^+\big\rangle + \big|\Psi^-\big\rangle\,\big) \qquad , \qquad |{-}{+}\rangle = \frac{1}{\sqrt{2}}\big(\,\big|\Psi^+\big\rangle - \big|\Psi^-\big\rangle\,\big)\ . \end{aligned} \tag{5.69}$$

We may use such a Bell basis for particles A and B or for particle B and C, or A and C. Here is the protocol :

- Alice prepares some state with her particle A :

$$|\chi\rangle_A = \alpha\,|+\rangle_A + \beta\,|-\rangle_A \ . \tag{5.70}$$

- Alice and Bob have agreed in advance on the definition of the Bell basis states and that Bob prepares the Bell state $|\Phi^+\rangle_{BC}$ with two particles B and C he has. Bob sends one of his two particle, say particle C to Alice.

- Alice now has particles A and C and "measures" the state of these two particles "against" the Bell basis of A and C. Technically this means that somehow there is an observable $O = x_1\,|\Phi^+\rangle\langle\Phi^+| + x_2\,|\Phi^-\rangle\langle\Phi^-| + x_3\,|\Psi^+\rangle\langle\Psi^+| + x_4\,|\Psi^-\rangle\langle\Psi^-|$ and, if the measurement of O yields x_i, the "reduction of the wave-packet" reduces the state to the corresponding Bell state. This measurement "destroys" Alice's state. She publicly announces to Bob the result of her measurement. Since there are only $4 = 2 \times 2$ possible outcomes, it only takes 2 classical bits to send this information to Bob.

- According to the information about Alice's measurement result, Bob acts on the state of his particle B with a certain unitary operator and then the state of his particle B will be identical to the initial state of Alice's particle A, namely $|\chi\rangle_B = \alpha\,|+\rangle_B + \beta\,|-\rangle_B$. We can say that the initial state $|\chi\rangle_A$ has been tele-transported to particle B.

This may look like magic, but it is just quantum mechanics with entangled states ! Let us see how this goes. To begin with the total state of the 3 particles $|\Psi\rangle$ is the tensor product of Alice's state $|\chi\rangle_A$ and the Bell state $|\Phi^+\rangle_{BC}$:

$$\begin{aligned}
|\Psi\rangle &= |\chi\rangle_A \otimes \big|\Phi^+\big\rangle_{BC} = \frac{1}{\sqrt{2}}\big(\alpha\,|+\rangle_A + \beta\,|-\rangle_A\big) \ \otimes \big(\,|{+}{+}\rangle_{BC} + |{-}{-}\rangle_{BC}\,\big) \\
&= \frac{1}{\sqrt{2}}\big(\alpha\,|{+}{+}{+}\rangle_{ABC} + \alpha\,|{+}{-}{-}\rangle_{ABC} + \beta\,|{-}{+}{+}\rangle_{ABC} + |{-}{-}{-}\rangle_{ABC}\,\big) \\
&= \frac{1}{\sqrt{2}}\big(\alpha\,|{+}{+}\rangle_{AC} + \beta\,|{-}{+}\rangle_{AC}\,\big) \otimes |+\rangle_B + \frac{1}{\sqrt{2}}\big(\alpha\,|{+}{-}\rangle_{AC} + \beta\,|{-}{-}\rangle_{AC}\,\big) \otimes |-\rangle_B \ .
\end{aligned} \tag{5.71}$$

Note the changed order AC and B in the last line. This writing dispays the part of the state accessible to Alice (the AC part) and the part accessible to Bob (the B part). We may further rewrite it by using the Bell basis for Alice's 2 particles A and C, using (5.69). This gives

$$\begin{aligned}
|\Psi\rangle &= \frac{1}{2}\Bigg[\Big(\alpha\big(\,\big|\Phi^+\big\rangle_{AC} + \big|\Phi^-\big\rangle_{AC}\,\big) + \beta\big(\,\big|\Psi^+\big\rangle_{AC} - \big|\Psi^-\big\rangle_{AC}\,\big)\Big) \otimes |+\rangle_B \\
&\qquad + \Big(\alpha\big(\,\big|\Psi^+\big\rangle_{AC} + \big|\Psi^-\big\rangle_{AC}\,\big) + \beta\big(\,\big|\Phi^+\big\rangle_{AC} - \big|\Phi^-\big\rangle_{AC}\,\big)\Big) \otimes |-\rangle_B\Big)\Bigg]
\end{aligned} \tag{5.72}$$

Now Alice does her "measurement against the Bell basis". It should be clear frrom the expression of this state that the 4 possible outcomes have equal probability $\big(\frac{1}{2}\big)^2\big(|\alpha|^2 + |\beta|^2\big) = \frac{1}{4}$. Suppose

Alice measures the value x_1 for the observable O defined above. Then the state gets projected with $|\Phi^+\rangle\langle\Phi^+|$ (and normalised) so that after the measurement the state is

$$|\widetilde{\Psi}_1\rangle = \alpha \left|\Phi^+\right\rangle_{AC} \otimes |+\rangle_B + \beta \left|\Phi^+\right\rangle_{AC} \otimes |-\rangle_B = \left|\Phi^+\right\rangle_{AC} \otimes \left(\alpha |+\rangle_B + \beta |-\rangle_B\right) . \tag{5.73}$$

But this means that after Alice's measurement the state of Bob's particle B is $\alpha |+\rangle_B + \beta |-\rangle_B$ which is exactly the initial state of Alice's particle A. Note that now Alice has the two particles A and C in the (entangled) Bell state and there is no way for her to recover her initial state for particle A, in agreement with the no-cloning theorem.

What if Alice's measurement has given x_2 so that the state would have been projected with $|\Phi^-\rangle$? Then

$$|\widetilde{\Psi}_2\rangle = \left|\Phi^-\right\rangle_{AC} \otimes \left(\alpha |+\rangle_B - \beta |-\rangle_B\right) . \tag{5.74}$$

All Bob then needs to do is to act on his state with the unitary operator $|+\rangle_B\langle+|_B - |-\rangle_B\langle-|_B$ (equivalent to σ_z) to recover Alice's initial state. Similarly, if Alice measures x_3 and projects with Ψ^+, Bob must act with σ_x and if she measures x_4, Bob must use $i\sigma_y$.

5.9 Quantum cryptography

Classical cryptography is based on the practical difficulty to decode the encoded message. The commonly used RSA encryption is based on a pair of private and public keys (e.g. two very large prime numbers). Suppose Alice has appropriately chosen a pair of keys. She publicly announces the value of the public key (but keeps the other key private) and anyone can encrypt a message using this public key through some agreed upon algorithm such that it is extremely difficult to retrieve the original message unless one possesses the second, private key. So Bob can encrypt his message, send it over an insecure channel to Alice who is the only one who can decrypt it with her private key. (Of course, Bob can still be tricked by Alix, who pretends she is Alice, into sending important information to the wrong person....)

Quantum cryptography, on the other hand, is based on a protocol where the sender (say, this is now Alice) first publicly could detect the presence of a spy before transmitting any important information. The protocol is based on the non-cloning theorem. Alice codes her message in a sequence of q-bits that are spin-$\frac{1}{2}$ particles (or actually photons) she sends to Bob. If a spy intercepts her particles and measures them to read the message, Bob and Alice will notice. The interception would go unnoticed if the spy could first duplicate each particle and do the measurements only on one of them. But this is impossible by the non-cloning theorem.

Suppose Alice uses a Stern-Gerlach type setup to prepare the particles and then sends a specific sequence of $|\pm\rangle_z$ to Bob. Of course, Bob should know that Alice has prepared her particles in eigenstates of S_z and he can use a Stern-Gerlach also oriented along the z-axis to determine the message. But if a spy who intercepts the message also knows that a z-basis is used, he can perfectly measure the z-component of each spin and then re-emit a particle in the same state as

measured. Then the spy would go undetected. We have seen that the non-cloning theorem was based on superpositions of orthogonal states. Indeed if the spy does not know the direction of Alice's Stern-Gerlach, he will choose a random direction to measure the spin. With respect to the eigenbasis of this random direction, Alice's states are superpositions, and then the non-cloning theorem applies.

Here is the protocol : Alice agrees with Bob (even publicly) that she uses a random sequence of x-basis eigenstates and z-basis eigenstates, sending e.g. 1000 particles to Bob. But she does not say which basis is used for each of the particles. Thus she sends a sequence like $\{|+\rangle_z, |-\rangle_z, |-\rangle_x, |+\rangle_z, |+\rangle_x, |-\rangle_z, |-\rangle_x, \ldots\}$. Bob measures the spins with his Stern-Gerlach, choosing randomly to orient it along the x or z-axis. If his axis coincides with the axis chosen by Alice, he finds, with probability one, $+\frac{\hbar}{2}$ if Alice sent $|+\rangle$ and he finds $-\frac{\hbar}{2}$ (with probability one) if Alice sent $|-\rangle$. We will simply say Bob finds $+$ or $-$. However, if Bob choses the wrong axis, half of the time he will find $+$ and half of the time he will find $-$ independently of what Alice had sent. The same applies to a spy who intercepts the sequence of particles, measures them and tries to re-emit the same state as measured. After having sent the 1000 particles, and after all the corresponding measurements by Bob, Bob tells Alice publicly which axis he has used for all his 1000 measurements and randomly choses 500 of them and tells Alice about his results. Among them should be an average of 250 where he used the same axis as Alice. Alice picks out these 250 measurements and checks if for these particles Bob's results all correspond (as they should) to the states she has sent. If a spy has intercepted the message, for about half of the 250 particles he will have used the wrong basis and re-emitted a particle that was not in the initial state, so that for about 125 particles Bob will not have measured what Alice has sent. Then Alice realises that the message has been intercepted. The probability that Bob measures the correct value for all 125 particles in the wrong state is totally negligible. Let's check this explicitly. Suppose Alice has sent $|+\rangle_z$ and the spy measures in the x direction. He has probability $\frac{1}{2}$ to find $+$ and probability $\frac{1}{2}$ to find $-$. If he finds $+$, he will re-emit a particle in the state $|+\rangle_x$ and Bob will then measure in the z-direction $+$ with probability $\frac{1}{2}$ and $-$ with probability $\frac{1}{2}$. Similarly if the spy has found $-$ and re-emitted a state $|-\rangle_x$. Of course, if the spy uses the correct basis, his presence goes undetected. Overall, for each intercepted particle there is a probability $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$ that Bob finds the wrong result and a probability $\frac{3}{4}$ that he finds the correct result. The probability that Bob finds the correct result for all 500 intercepted particles is $\left(\frac{3}{4}\right)^{500} = e^{-500\ln(4/3)} \simeq e^{-500/3} \simeq e^{-167}$ which is indeed extremely small ! On the other hand, if Alice concludes that there is no spy, from the remaining 500 particles (for which Bob has not told anybody of his result) she chooses those for which Bob has used the same axis as she did (about 250) and composes her message by telling Bob publicly to use his measurement results in a certain order, e.g. measurement no 7, 19, 489, 245, 72, 46, etc. This provides for Bob the desired message $+-++--\ldots$. Of course, all this is useless if the spy manages to make Alice believe he is Bob...

5.10 Density operators on tensor product spaces and reduced density operators

In subsection 2.10, we have discussed the description of a quantum mechanical system in terms of the density operator rather than in terms of a state vector $|\psi\rangle$. We may define the density operator for a system in the tensor product space in exactly the same way. If $|\Psi\rangle$ is a general state in $\mathcal{H}_{(1)} \otimes \mathcal{H}_{(2)}$ then $\rho = |\Psi\rangle \langle\Psi|$ and for a statistical mixture of $|\Psi_i\rangle$ with statistical probabilities p_i we have $\rho = \sum_i p_i |\Psi_i\rangle \langle\Psi_i|$.

Often we want to do only measurements on one of the two subsystems, corresponding to observables A acting in $\mathcal{H}_{(1)}$ only. One can then work with a reduced density matrix $\rho_{(1)}$ which is a linear operator on $\mathcal{H}_{(1)}$, obtained by doing the partial trace over $\mathcal{H}_{(2)}$. This is done as follows. Let $\{|\chi_n\rangle\}$ be a basis of $\mathcal{H}_{(1)}$ and $\{|\varphi_m\rangle\}$ be a basis of $\mathcal{H}_{(2)}$. Then $\{|\chi_n\rangle \otimes |\varphi_m\rangle\}$ is a basis of $\mathcal{H}_{(1)} \otimes \mathcal{H}_{(2)}$. The operator $\rho_{(1)}$ is completely specified if we give its matrix elements in the $\{|\chi_n\rangle\}$ basis. They are defined as

$$\langle\chi_k| \rho_{(1)} |\chi_n\rangle = \sum_m \langle\chi_k| \otimes \langle\varphi_m| \rho |\chi_n\rangle \otimes |\varphi_m\rangle \ . \tag{5.75}$$

Since we have the "same" bra $\langle\varphi_m|$ and ket $|\varphi_m\rangle$ on both sides, we write

$$\rho_{(1)} = \sum_m \langle\varphi_m|_2 \ \rho \ |\varphi_m\rangle_2 = \ \mathrm{tr}_{(2)} \, \rho \ , \tag{5.76}$$

with the obvious notation that $|\varphi_m\rangle_2$ means that this ket refers to the Hilbert space $\mathcal{H}_{(2)}$, and $\mathrm{tr}_{(2)}$ is the *partial trace* over the $\mathcal{H}_{(2)}$.

In subsection 5.5 we have discussed how to describe measurements on one of the two systems, in particular the probability that the measurement of an observable A pertaining to the first system gives a_n was given in (5.39) as $\mathcal{P}_{(1)}(a_n, \Psi) = \langle\Psi| P_{(1)}(a_n) |\Psi\rangle$ with the projector $P_{(1)}(a_n) = \Big(\sum_{i=1}^{d_n} |\phi_n^i\rangle \langle\phi_n^i| \Big) \otimes \mathbf{1} = P(a_n) \otimes \mathbf{1}$, cf. (5.37). This is now written as

$$\begin{aligned} \mathcal{P}_{(1)}(a_n, \Psi) &= \mathrm{tr} \, \rho \, P_{(1)}(a_n) = \sum_{k,m} \langle\chi_k| \otimes \langle\varphi_m| \ \rho \ \Big(P(a_n) \otimes \mathbf{1} \Big) |\chi_k\rangle \otimes |\varphi_m\rangle \\ &= \sum_k \langle\chi_k|_1 \Big(\sum_m \langle\varphi_m|_2 \ \rho |\varphi_m\rangle_2 \Big) P(a_n) |\chi_k\rangle_1 \\ &= \mathrm{tr}_1 \ \rho_{(1)} P(a_n) \end{aligned} \tag{5.77}$$

We see that the probabilities of measurements on the subsystem 1 can be described in terms of the reduced density operator ρ_1 for this subsystem 1, and similarly for the subsystem 2. Of course, the corresponding result for the mean value of A immediately follows by multiplying with a_n and summing over n ($\sum_n P(a_n) a_n = A$) :

$$\langle\langle A \rangle\rangle = \ \mathrm{tr} \, \rho (A \otimes \mathbf{1}) = \ \mathrm{tr}_1 \, \rho_{(1)} A \ . \tag{5.78}$$

Let us now describe what happens if we start with a pure state[29] in the tensor product space. This can be either a factorised state $\big|\psi_{(1)}\big\rangle \otimes \big|\psi_{(2)}\big\rangle$ or an entangled state $|\Psi\rangle$ like the singlet state made from two spin-$\frac{1}{2}$. In the first case, $\rho = \big|\psi_{(1)}\big\rangle\big\langle\psi_{(1)}\big| \otimes \big|\psi_{(2)}\big\rangle\big\langle\psi_{(2)}\big|$ and then

$$\begin{aligned}\rho_1 &= \mathrm{tr}_2\ \rho = \sum_m \big|\psi_{(1)}\big\rangle\big\langle\psi_{(1)}\big|\,\langle\varphi_m\,\big|\psi_{(2)}\big\rangle\big\langle\psi_{(2)}\big|\,\varphi_m\rangle = \big|\psi_{(1)}\big\rangle\big\langle\psi_{(1)}\big|\ \big\langle\psi_{(2)}\big|\Big(\sum_m |\varphi_m\rangle\langle\varphi_m|\Big)\big|\psi_{(2)}\big\rangle \\ &= \big|\psi_{(1)}\big\rangle\big\langle\psi_{(1)}\big|\ , \end{aligned} \tag{5.79}$$

as expected. This is again the density operator of a pure state. However, if we start with an entangled state the result will not be a density operator corresponding to a pure state. Let us exemplify this for the singlet state where

$$\rho = |0,0\rangle\langle 0,0| = \frac{1}{2}\Big(\,|+-\rangle\langle+-| - |+-\rangle\langle-+| - |-+\rangle\langle+-| + |-+\rangle\langle-+|\,\Big) \tag{5.80}$$

Then

$$\rho_1 = \mathrm{tr}_2\ \rho = \langle+|_2\,\rho\,|+\rangle_2 + \langle-|_2\,\rho\,|-\rangle_2 = \frac{1}{2}\big(\,|-\rangle_1\langle-|_1 + |+\rangle_1\langle+|_1\,\big) = \frac{1}{2}\,\mathbf{1}_{(1)}\ , \tag{5.81}$$

and the reduced density matrix on $\mathcal{H}_{(1)}$ simply is $\frac{1}{2}$ times the identity operator. Hence it has two eigenvalues equal to $\frac{1}{2}$, and so it cannot correspond to any pure state. This is a general feature : taking the partial trace of a pure-state density operator for an entangled state results in a mixed state.

5.11 ZX-calculus

We have just introduced the notation where the subscript on a ket or bra indicates the (individual) Hilbert space the ket or bra is in. In particular then $\langle+|_2\,|-+\rangle \equiv \langle+|_2\,|-+\rangle_{12} = |-\rangle_1$ is a ket in the first Hilbert space. If we have multiple tensor products of, say 6, Hilbert spaces, $\otimes_{i=1}^6 \mathcal{H}_{(i)}$, then we can similarly use the notation $\langle+-+|_{134}\,|++-+--\rangle_{123456} = |+--\rangle_{256}$, etc. One can also consider objects like $|+--\rangle_{245}\langle--+-|_{1456}$. Of course, this is not a linear operator on $\otimes_{i=1}^6 \mathcal{H}_{(i)}$, (but it is a linear operator from a four-fold tensor product of spin-$\frac{1}{2}$ Hilbert spaces to a three-fold tensor product of such spaces), and we may compose two such objects as

$$\Big(\,|+--\rangle_{245}\langle--+-|_{1456}\,\Big) \otimes \Big(\,|-++\rangle_{136}\langle-+|_{23}\,\Big)\ , \tag{5.82}$$

and this is now a linear operator on $\otimes_{i=1}^6 \mathcal{H}_{(i)}$. The object $|+--\rangle_{245}\langle--+-|_{1456}$ could be represented graphically as something that has 4 inputs (for the particles 1456) and 3 outputs (for the particles 245). In a graphical representation one could draw a blob with 4 incoming lines and three outgoing ones. So this looks (almost) like a spider, and that's what we will call it.

[29] Recall that "pure state" means that quantum mechanically there is a single state $|\Psi\rangle$ which can be either factorised or entangled. "Pure" is used in opposition to "mixed" which refers to a statistical mixture.

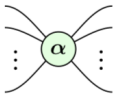
We will now describe an even simpler class of spiders and corresponding composition rules that lead to the so-called ZX-diagrams and ZX-calculus. ZX-calculus is a powerful graphical language that is very useful to describe quantum circuits, establish equivalences between different looking circuits, and, hence, to perform quantum circuit simplification.[30]

A ZX-diagram is composed of lines and vertices where lines meet. The lines are directed, and can be labelled as incoming or outgoing, which can be made clear by putting arrows on the lines. (As we will see soon, the arrows on the internal lines, i.e. between two vertices, will turn out to be irrelevant.) There are two types of vertices, called the X-spider and the Z-spider. Each spider is labelled by an angle (phase) defined modulo 2π and we will take $\alpha \in (-\pi, \pi]$. A given spider has a certain number k of lines coming in (usually drawn as coming in from the left) and a certain number of lines l going out (usually drawn as going out to the right). The numbers k and l are also called in- and out-arities. We can thus label these spiders as $[X, \alpha, k, l]$ or $[Z, \alpha, k, l]$. In colour drawings, the X-spiders are drawn as red dots and the Z-spiders as green dots.

Now, one considers that each line corresponds to a qbit (spin $\frac{1}{2}$) and each spider with k incoming and l outgoing lines will represent a certain linear map from the k-fold tensor product of spin-$\frac{1}{2}$ Hilbert spaces to the l-fold product of such spaces. To write them out we need two different basis' of the single spin-$\frac{1}{2}$ (single qbit) Hilbert space. These are $|\pm\rangle_z$ and $|\pm\rangle_x$. In this subsection we will instead adopt the standard notation from quantum computing where the "computational basis" is the z-basis with $|0\rangle \equiv |+\rangle_z$ and $|1\rangle \equiv |-\rangle_z$, and the x-basis is denoted as $|+\rangle \equiv |+\rangle_x$ and $|-\rangle \equiv |-\rangle_x$. Actually it does not matter how these basis' correspond to the spin eigenstates. The only things that matter is that $\{|0\rangle, |1\rangle\}$ is one orthonormal basis, and that $\{|+\rangle, |-\rangle\}$ is another orthonormal basis and that the inner products between the elements of one basis and those of the other basis are *real* and given by

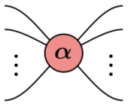
$$\langle 0|+\rangle = \langle 1|-\rangle = \langle 0|-\rangle = \frac{1}{\sqrt{2}} \quad , \quad \langle 1|-\rangle = -\frac{1}{\sqrt{2}} \, . \tag{5.83}$$

This makes clear that there is a total symmetry upon switching the roles of the two basis'. Then the spiders are defined as



$$= [Z, \alpha, k, l] = |0 \ldots 0\rangle_{12\ldots l} \langle 0 \ldots 0|_{12\ldots k} + e^{i\alpha} |1 \ldots 1\rangle_{12\ldots l} \langle 1 \ldots 1|_{12\ldots k} \, , \tag{5.84}$$

and



$$= [X, \alpha, k, l] = |+ \ldots +\rangle_{12\ldots l} \langle + \ldots +|_{12\ldots k} + e^{i\alpha} |- \ldots -\rangle_{12\ldots l} \langle - \ldots -|_{12\ldots k} \, . \tag{5.85}$$

[30] R. Duncan, A. Kissinger, S. Perdrix and J. van de Wetering, *Graph-theoretic simplification of quantum circuits with the ZX-calculus*, arXiv:1902.03178 [quant-ph]. The more professionally looking figures in this subsection are borrowed from this paper.

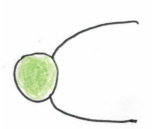
The bras and kets in these definitions are completely symmetric under permutation of the particle labels, and eventually the particle number labels will turn out to be unnecessary. By convention, if the phase is zero, it is simply not written.

This means that we do not need to indicate the labels of the qbits on which the spiders acts. Note also that for $k = 0$ these spiders just represent certain kets, while for $l = 0$ they represent certain bras. For $k = 0,\ l = 1$, both $[X, \alpha, 0, 1]$ and $[Z, \alpha, 0, 1]$ have a single outgoing line and correspond to a single qbit state or ket, in particular

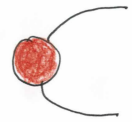
$$= [Z, 0, 0, 1] = |0\rangle + |1\rangle = \sqrt{2}\,|+\rangle \quad , \quad [Z, \pi, 0, 1] = |0\rangle - |1\rangle = \sqrt{2}\,|-\rangle \ , \tag{5.86}$$

$$= [X, 0, 0, 1] = |+\rangle + |-\rangle = \sqrt{2}\,|0\rangle \quad , \quad [X, \pi, 0, 1] = |+\rangle - |-\rangle = \sqrt{2}\,|1\rangle \ . \tag{5.87}$$

An analogous statement holds for $k = 1,\ l = 0$ and corresponding bras. Since a quantum state corresponds to a ray, we will consider any overall non-vanishing complex ("scalar") factor as irrelevant. Similarly, one finds that $[X, 0, 0, 2] = |{+}{+}\rangle + |{-}{-}\rangle$. But expressing this in the other basis one easily sees that it equals $|00\rangle + |11\rangle$. This is the Bell state $|\Phi^+\rangle$ we defined earlier. In any case,



$$= [Z, 0, 0, 2] = |00\rangle + |11\rangle = |{+}{+}\rangle + |{-}{-}\rangle = [X, 0, 0, 2] =$$

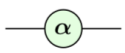


. (5.88)

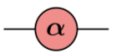
Let us look a bit more closely at the spiders $k = l = 1$. They are linear maps acting on a single qbit, i.e. a single spin-$\frac{1}{2}$. Let us recall from (3.49) the expressions of the unitary rotation operators $U(\alpha, x)$ and $U(\alpha, z)$ acting on single spin-$\frac{1}{2}$ states, which can be rewritten in our current notation as

$$\begin{aligned} U(\alpha, z) &= \cos\frac{\alpha}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) - i\sin\frac{\alpha}{2}\left(|0\rangle\langle 0| - |1\rangle\langle 1|\right) = e^{-i\frac{\alpha}{2}}\,|0\rangle\langle 0| + e^{i\frac{\alpha}{2}}\,|1\rangle\langle 1| \\ U(\alpha, x) &= \cos\frac{\alpha}{2}\left(|+\rangle\langle +| + |-\rangle\langle -|\right) - i\sin\frac{\alpha}{2}\left(|+\rangle\langle +| - |-\rangle\langle -|\right) = e^{-i\frac{\alpha}{2}}\,|+\rangle\langle +| + e^{i\frac{\alpha}{2}}\,|-\rangle\langle -| \ . \end{aligned} \tag{5.89}$$

Comparing with the definitions of the Z and X spiders we see that



$$= [Z, \alpha, 1, 1] = e^{i\frac{\alpha}{2}}\ U(\alpha, z) \quad ,$$

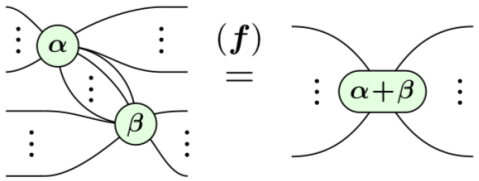


$$= [X, \alpha, 1, 1] = e^{i\frac{\alpha}{2}}\ U(\alpha, x)\ . \tag{5.90}$$

Hence, up to the irrelevant phase $e^{i\frac{\alpha}{2}}$, we may identify $[Z, \alpha, 1, 1]$ with the rotation by α around the z-axis as given by $U(\alpha, z)$, and similarly $[X, \alpha, 1, 1]$ with the rotation by α around the x-axis as given by $U(\alpha, x)$. Recall also (3.50), which showed that the rotation operator $U(\alpha, y)$ around the y-axis could be obtained by composing rotations around the x and z-axis'. This is the reason why there is no need to introduce a spider $[Y, \alpha, 1, 1]$ and any linear map acting on a single qbit (up to

an overall factor) can be obtained by composing the X and Z-spiders. What is more surprising is the fact (which we will not prove) that an arbitrary linear map from the k qbit Hilbert space to the l qbit Hilbert space can be obtained by composing the different X and Z-spiders $[X, \alpha', k', l']$ and $[Z, \alpha'', k'', l'']$ into some (possibly complicated) ZX-diagram. When drawing ZX-diagrams one must be careful about the order since we identify the spiders with the corresponding operators and operators are composed from right to left, while the ZX-diagram is conventionally drawn with the incoming lines on the left and the outgoing lines on the right.

One can then show several equivalence ("rewrite") rules about the ZX-diagrams. A first simple rule is the fusion rule depicted as



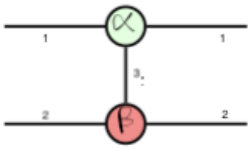
(5.91)

which follows trivially from the fact that the two Z-spiders are given in the same orthonormal basis. To see this, consider the example where the first Z-spider ($[Z, \alpha, ...]$) has 1 incoming line (qbit 1) and two outgoing lines (qbits 1 and 3), and the second Z-spider (($[Z, \beta, \ldots]$) has two incoming lines (qbits 2 and 3) and one outgoing line (qbit 2). Then the diagram on the left corresponds to

$$\begin{aligned}
[Z,\beta,2,1]_{2|23}[Z,\alpha,1,2]_{13|1} &= \left(\ |0\rangle_2 \langle 00|_{23} + e^{i\beta} |1\rangle_2 \langle 11|_{23} \ \right)\left(\ |00\rangle_{13} \langle 0|_1 + e^{i\alpha} |11\rangle_{13} \langle 1|_1 \ \right) \\
&= |0\rangle_2 \langle 00|_{23} \ |00\rangle_{13} \langle 0|_1 + e^{i\alpha} e^{i\beta} |1\rangle_2 \langle 11|_{23} \ |11\rangle_{13} \langle 1|_1 \\
&= \langle 0|0\rangle |0\rangle_2 \langle 0|_2 \ |0\rangle_1 \langle 0|_1 + e^{i\alpha+i\beta} \langle 1|1\rangle |1\rangle_2 \langle 1|_2 |1\rangle_1 \langle 1|_1 \\
&= |00\rangle_{12} \langle 00|_{12} + e^{i\alpha+i\beta} |11\rangle_{12} \langle 11|_{12} \\
&= [Z,\alpha+\beta,2,2]_{12|12} \ ,
\end{aligned} \tag{5.92}$$

A most important rule is that the ZX-diagrams are topologically invariant, by which we mean that we can move the spiders around and bend the internal lines, as long as we keep fixed the external lines (that go into and out of the diagram) including their labels $1, \ldots k$ and $1, \ldots l$. Then, as we move the spiders around, an internal line that was outgoing from the i^{th} spider and ingoing into the j^{th} spider can be changed into an internal line that is outgoing from the j^{th} spider and ingoing into the i^{th} spider. This will occur precisely if initially the i^{th} spider was to the left of the j^{th} spider and will be moved to the right of it. Let us assign a label to the qbit corresponding to the internal line, say n. Then, before the move, this internal line gives rise to an inner product of the form $\langle t|_n |v\rangle_n = \langle t|v\rangle$, while after the move there will be corresponding inner products $\langle v|_n |t\rangle_n = \langle v|t\rangle$. The important property is that all these inner products are real because we only use the z and the x-basis, and then $\langle v|t\rangle = \langle t|v\rangle$.

Let's look at an example corresponding to the following figure where the upper line corresponds to the qbit labelled 1, the lower line to the qbit labelled 2 and the internal line is labelled by 3.

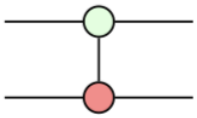


Consider first the situation where the green Z-spider is to the left of the red X-spider in the diagram. This means that the green Z-spider "acts first" and only then acts the red X-spider. This translates into the operator order $[X,\beta,2,1]_{2|23}[Z,\alpha,1,2]_{13|1}$. On the other hand, if we draw the green Z-spider to the right of the red X-spider this means that the red X-spider "acts first" and only then acts the green Z-spider. This translates into the operator order $[Z,\alpha,2,1]_{1|13}[X,\beta,1,2]_{23|2}$.

Exercise : *Show that both expressions are equal to each other and equal to*

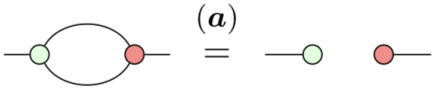
$$[X,\beta,2,1]_{2|23}[Z,\alpha,1,2]_{13|1} = [Z,\alpha,2,1]_{1|13}[X,\beta,1,2]_{23|2}$$
$$= \frac{1}{\sqrt{2}}\big(\ |0+\rangle_{12}\langle 0+|_{12} + e^{i\alpha}\,|1+\rangle_{12}\langle 1+|_{12} + e^{i\beta}\,|0-\rangle_{12}\langle 0-|_{12} - e^{i\alpha+i\beta}\,|1-\rangle_{12}\langle 1-|_{12}\ \big)\ . \qquad (5.93)$$

Note that this is a linear map from a 2 qbit Hilbert space to itself, and for any fixed basis it can be viewed as a $2^2\times 2^2$-matrix. While the above form is the most compact one, one might want to use the same basis, e.g. $\{|0\rangle, |1\rangle\}$, for both incoming (and outgoing) qbits. It is straightforward to express the $|\pm\rangle$ and $\langle\pm|$ in this basis, resulting in a total of 16 terms. For $\alpha=\beta=0$, however, most terms vanish and the expression simplifies and we get what is known as CNOT-gate:



$$= \frac{1}{\sqrt{2}}\big(\ |00\rangle\langle 00|+|01\rangle\langle 01|+|10\rangle\langle 11|+|11\rangle\langle 10|\ \big) \simeq \frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\ . \qquad (5.94)$$

Exercise : *Show similarly the so-called antipodal rule*



$$:\quad [X,0,2,1]\,[Z,0,1,2] \simeq [X,0,0,1][Z,0,1,0]\ . \qquad (5.95)$$

There are other transformation rules which we will not mention here. But there are proofs about which set of transformation rules (rewrite rules) is the minimal set so that any two ZX-diagrams that describe the same linear map on the multiple qbit states can always be transformed into each other by these graphical rewrite rules. This provides a powerful method for quantum circuit simplification.