Quantum optics

Jacopo Tissino

May 12, 2020

Wed Jan 08 2020

Course given for the SGSS by professors Paolo Villoresi and Giuseppe (Pino) Vallone.

The work of the team on quantum communication started in 2003, now there is a lot of interest on it.

The aim of this course is to discuss the *implementation* of the concepts in quantum information. The field is relatively young: anyone working on it needs to work with both theory and experiment.

Quantum information comes from merging information theory and quantum theory.

References:

1. "Introductory quantum optics", Gerry & Knight;
2. "Quantum metrology, imaging, and communication", Simon, Jaeger, ...
3. Lebellac, "Quantum Physics"

add references from slides

Bell inequalities: 1964, no physical theory of local hidden variables can ever reproduce all the predictions of quantum mecnanics.

There are quantum experiments with relativistic distances and speeds.

In 2016 there was a Quantum Manifesto.

1 Meet the photon

A complete explanation of the photoelectric effect was given by Einstein. He pointed out the difference in approaches at his time between the atomic theory of matter and the continuous functions representing light in Maxwell's theory.

We follow Gerry & Knight for the quantization of the EM field.

We start from the vacuum Maxwell equations:

$$\nabla \times E = -\frac{\partial B}{\partial t} \tag{1}$$

$$\nabla \times B = \mu_0 \epsilon_0 \frac{\partial E}{\partial t} \tag{2}$$

$$\nabla \cdot B = 0 \tag{3}$$

$$\nabla \cdot E = 0\,, \tag{4}$$

and seek trigonometric solutions in a box-shaped cavity: they look like

$$E_x(z,t) = \left(\frac{2\omega^2}{V\epsilon_0}\right)^{1/2} \sin(kz) q(t)\,, \tag{5}$$

where $k = \omega/c$. If we fix the boundary conditions of $E_x(0,t) = E_x(L,t) = 0$ we find $k = m\pi/L$.

Here V is the volume of our cavity. The magnetic field corresponding to this is

$$B_y(z,t) = \left(\frac{\mu_0\epsilon_0}{k}\right)\left(\frac{2\omega^2}{V\epsilon_0}\right)^{1/2} \dot{q}(t)\cos(kz)\,, \tag{6}$$

where $\dot{q}$ corresponds precisely to the conjugate momentum to q: $\dot{q} = p$.

Then, the Hamiltonian can be shown to be

$$H = \frac{1}{2}\int \mathrm{d}V \left(\epsilon_0 E^2 + \frac{B^2}{\mu_0}\right) = \frac{1}{2}\left(p^2 + \omega^2 q^2\right). \tag{7}$$

In order to quantize the field, we use the correspondence principle to replace $p \to \hat{p}$ and $q \to \hat{q}$. These are Hermitian operators acting on the space $L^2(V)$ and thus correspond to observables, their commutator is $[\hat{q}, \hat{p}] = i\hbar$.

Now, we can introduce the creation and annnihilation operators:

$$\hat{a} = \frac{1}{\sqrt{2\hbar\omega}}\left(\omega\hat{q} + i\hat{p}\right) \tag{8}$$

$$\hat{a}^\dagger = \frac{1}{\sqrt{2\hbar\omega}}\left(\omega\hat{q} - i\hat{p}\right), \tag{9}$$

and their product will give the number operator: $\hat{N} = \hat{a}^\dagger\hat{a}$. These are not Hermitian and thus not observable.

Then, we have

$$\hat{E}_x = \mathcal{E}_0\left(\hat{a} + \hat{a}^\dagger\right)\sin(kz) \tag{10}$$

$$\hat{B}_y = -i\mathcal{B}_0\left(\hat{a} - \hat{a}^\dagger\right)\cos(kz)\,, \tag{11}$$

for some normalization.

The Hamiltonian is given by $\hat{H} = \hat{N} + 1/2$.

The time-evolution in the Heisenberg picture of the creation and annihilation operators can be shown to be given by

$$\frac{\mathrm{d}\hat{a}}{\mathrm{d}t} = \frac{i}{\hbar}[\hat{H}, \hat{a}] = -i\omega\hat{a}\,, \tag{12}$$

so the evolution is given by circular motion.

If $|n\rangle$ is an eigenvector of $\hat{H}$ with energy E_n, then $\hat{a}^\dagger |k\rangle$ is an eigenvector with energy $E_n + \hbar\omega$. Then it is clear why this operator is called a creation operator: it *creates* a quantum of energy.

Similarly, $\hat{a}$ decreases the energy by $\hbar\omega$. The ground state is the one for which $\hat{a}\,|\psi\rangle = 0$, it is called $|0\rangle$ and has energy $\hbar\omega/2$. This is *zero-point energy*.

This ground state must exist since the eigenvalues of $\hat{N}$ must be positive.

The interpretation for this is then the fact that the excitation number gives us the number of photons in the cavity. We can do some calculations to show that the normalization we need in order to retain a normalized vector when applying the creation operator to the state $|N\rangle$ is $1/\sqrt{N+1}$, since

$$\hat{a}^\dagger |n\rangle = \sqrt{n+1}\,|n\rangle\ , \tag{13}$$

so we get a formula for a generic state starting from the ground state:

$$|n\rangle = \frac{(\hat{a}^\dagger)}{\sqrt{n!}}|0\rangle\ . \tag{14}$$

We can find eigenbases $|i\rangle$ from these operators, and write completeness relations:

$$\sum_i |i\rangle\langle i| = \mathbb{1}\,. \tag{15}$$

The only nonzero matrix elements of the creation and annihilation operators are the ones which are just off-diagonal by one in the basis of the Hamiltonian.

Fri Jan 10 2020

The energy of the states $|n\rangle$ is well defined, but there are still issues to sort out: for instance, the expectation value of the electric field is zero *at each point*,

$$\langle n|\, E_x(z,t)\,|n\rangle \propto \langle n|\,\hat{a}\,|n\rangle + \langle n|\,\hat{a}^\dagger\,|n\rangle = 0\,. \tag{16}$$

However, the expectation value of the *square* of the electric field is nonzero:

$$\left\langle E_x^2(z,t)\right\rangle = 2\mathcal{E}_0^2\sin^2(kz)\left(n+\frac{1}{2}\right). \tag{17}$$

This is in accordance with the uncertainty principle, since the operator $\hat{n}$ does not commute with the electric field operator $\hat{E}_x$. We can write the undetermination relation

$$\Delta n \Delta E \geq \frac{1}{2}\mathcal{E}_0\left|\sin(kz)\right|\left|\left\langle \hat{a}^\dagger - \hat{a}\right\rangle\right|. \tag{18}$$

We expect to be able to find a notion of phase such that there is a number-phase uncertainty relation, similarly to the time-energy uncertainty relation.

The time evolution of the electric field operator is given by

$$E_x = \mathcal{E}_0\left(\hat{a}e^{-i\omega t} + \hat{a}^\dagger e^{i\omega t}\right)\sin(kz)\,, \tag{19}$$

and we define the quadrature operators:

$$X_1 = \frac{1}{2}\left(\hat{a} + \hat{a}^\dagger\right) \qquad \text{and} \qquad X_2 = \frac{1}{2i}\left(\hat{a} - \hat{a}^\dagger\right). \tag{20}$$

We have effectively decomposed the electric field into two oscillating parts, out of phase with each other by 90°. We have the commutator $[\hat{X}_1, \hat{X}_2] = i/2$. Even for the vacuum state the fluctuations of these operators are nonzero.

We will now distinguish two different kinds of radiation: blackbody radiation and coherent (laser-like) radiation.

For the first case, we know that the distribution of the energy levels is given by the Boltzmann distribution,

$$P(n) = \frac{1}{Z}\exp\left(-\frac{E_n}{k_B T}\right), \tag{21}$$

where Z is a normalization factor. We now give an intuitive justification.

Let us suppose that we have a system of four particles, with three quanta of energy, which we write as ΔE. How can this energy be distributed?

0	ΔE	$2\Delta E$	$3\Delta E$	$4\Delta E$	Possibilities
3	0	0	1	0	4
2	1	1	0	0	12
1	3	0	0	0	4

So, for $0\Delta E$ we have $12 + 24 + 4 = 40$ total possibilities, for $1\Delta E$ we have $12 + 12 = 24$ total possibilities, for $2\Delta E$ we have 12 possibilities, for $3\Delta E$ we have 4 possibilities. The total is then 80.

This kiind of looks like an exponential decrease, I guess if we were to do a more precise calculation we would get an exponential exactly.

In a quantum setting, we will have a density matrix looking like

$$\rho = \frac{1}{\operatorname{tr}\exp\left(-\hat{H}/k_B T\right)}\exp\left(-\hat{H}/k_B T\right); \tag{22}$$

which gives a familiar result:

$$\rho = \sum_n \frac{\exp(-E_n/k_B T)}{Z}\,|n\rangle\langle n|\,. \tag{23}$$

The average number of photons can be found to be given by

$$\langle n \rangle = \frac{1}{\exp(\hbar\omega/k_B T) - 1} \,. \tag{24}$$

In the limits $\hbar\omega/k_B T$ going to either infinity or zero we get $\langle n \rangle \to \hbar\omega/k_B T$ or its inverse.

We can write the relation

$$\exp(-\hbar\omega/k_B T) = \frac{\overline{n}}{1+\overline{n}} \,, \tag{25}$$

where $\overline{n} = \langle n \rangle$. Then we will have

$$\rho = \frac{1}{1+\overline{n}} \sum_n \left(\frac{\overline{n}}{1+\overline{n}} \right)^n |n\rangle\langle n| \,. \tag{26}$$

It can be shown that

$$\left\langle \hat{n}^2 \right\rangle = \overline{n} + 2\overline{n}^2 \,, \tag{27}$$

which implies

$$\Delta n = \left(\overline{n} + \overline{n}^2 \right)^{1/2} , \tag{28}$$

so we have $\Delta n \sim \overline{n} + \frac{1}{2}$ asymptotically. Therefore, there never is a well-defined number of photons in the box.

We can write an expression for the average energy density $U(\omega)$:

$$U(\omega) = \frac{\hbar\omega^3}{\pi^2 c^3} \frac{1}{\exp(\hbar\omega/k_B T) - 1} \,. \tag{29}$$

The average energy of these photons is given by $\hbar\omega\overline{n}$.

From these expressions we can recover Wien's law and Stefan-Boltzmann's law.

How do we represent a plane wave in a QFT? If we want a nonzero electric field we need a superposition of number states differing by ± 1.

Another way to put it is: are there eigenstates $|\alpha\rangle$ of the annihilation operator $\hat{a}$?

They will look like

$$|\alpha\rangle = C_0 \sum_n \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,. \tag{30}$$

By normalization, $C_0 = \exp\left(-|\alpha|^2/2\right)$. This gives us a coherent state, which like we wanted has a nonzero expected electric field. It looks precisely like a plane wave:

$$\left\langle \hat{E}_x \right\rangle_\alpha = i\sqrt{\frac{\hbar\omega}{2\epsilon_0 V}} \left(\alpha \exp\left(i\vec{k} \cdot \vec{x} - i\omega t \right) - \alpha^* \exp\left(-i\vec{k} \cdot \vec{x} + i\omega t \right) \right) . \tag{31}$$

We find also the expectation value of the *square* of the electric field

$$\left\langle E_x^2 \right\rangle_\alpha = \frac{\hbar\omega}{2\epsilon_0 V}\left(1 + 4|\alpha|^2 \sin^2(\omega t - \vec{k}\cdot\vec{r} - \theta)\right), \tag{32}$$

where $\alpha = |\alpha| \exp(i\theta)$.

This means that not even in the vacuum state we can have a zero expected electric field. The vectors $|\alpha\rangle$ are *over-complete*, since they are bidimensional while a one-dimensional continuous basis would be enough to span the Hilbert space.

The average of the number of photons $\hat{n}$ for an eigestate $|\alpha\rangle$ is quickly calculated to be $|\alpha|^2$: then we can see that $|\alpha|^2 = \overline{n}$.

So, with these states we have $\left\langle \hat{n}^2 \right\rangle_\alpha = \overline{n}^2 + \overline{n}$. Therefore $\Delta n = \sqrt{\overline{n}}$. The probability of detecting n photons is given by $\left|\langle n|\alpha\rangle\right|^2$:

$$P_\alpha(n) = \exp(-\overline{n})\frac{\overline{n}^n}{n!}, \tag{33}$$

a Poissonian distribution. If the number of photons gets large then the Poissonian approaches a Gaussian.

Mon Jan 13 2020

The distribution for a thermal source is more irregular than the Poissonian we get for the coherent light.

Recall: our coherent states are given by

$$|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right)\sum_n \frac{\alpha^n}{\sqrt{n!}}|n\rangle \tag{34}$$

where $|n\rangle$ are the number eigenstates.

We can define the displacement operator:

$$\hat{D}(\alpha) = \exp\left(\alpha\hat{a}^\dagger - \alpha^*\hat{a}\right), \tag{35}$$

which, it can be proven, can give us the state $|\alpha\rangle$ starting from the vacuum $|0\rangle$: $\hat{D}(\alpha)|0\rangle = |\alpha\rangle$.

We discuss interactions with an electromagnetic field: we have the interaction term in the Hamiltonian:

$$\hat{V}(t) = \int \mathrm{d}^3 r\, \vec{j}(\vec{r},t)\cdot\hat{A}(\vec{r},t), \tag{36}$$

where $\hat{A}$ is the operator corresponding to the vector potential, and is given by

$$\hat{A} = . \tag{37}$$

In certain cases, we can only consider the dipole contribution since on the length scales of the problem the field is approximately constant.

...

We can find an expression for α by integrating a coupling term. The coherent states are not orthonormal: we have

$$\langle\beta|\alpha\rangle = \exp\left(\frac{1}{2}\left(\beta^*\alpha - \beta\alpha^* - \left|\beta-\alpha\right|^2\right)\right), \tag{38}$$

which can never be zero: its square norm is $\exp\left(-\left|\beta-\alpha\right|^2\right)$ there are no orthogonal vectors here. Nevertheless, we are in a Hilbert space so we can write a completeness relation, even though we do *not* have a basis.

We have a distribution in the space of α: it is constrained by the uncertainty principle. We can use *homodyne* detectors to select a quadrature to "squeeze" and get more resolution on. *Heterodyne* means we split the signal and use both.

We can use our QFT of light to solve the problem of the interaction of an EM field with an atom: the transformed Hamiltonian is

$$H' = \frac{1}{2m}\left(\vec{P} + e\vec{A}\right)^2 + V - e\Phi\,, \tag{39}$$

which is an operator equation, even though I omit the hats.

If we consider both the Hilbert spaces, we will have a transition from an initial state $|a\rangle\,|n\rangle$ to either $|b\rangle\,|n+1\rangle$ if a photon is emitted or to $|b\rangle\,|n-1\rangle$ if a photon is absorbed.

We compute the probability amplitudes of these by sandwitching the interaction Hamiltonian.

The zero-point energy cannot be harvested for a transition: however, spontaneous emission can happen by interaction with the vacuum of the EM field.

The interaction Hamiltonian is separable: its EM part is either $\hat{a}$ or $\hat{a}^\dagger$, so we immediately get the result that

$$\frac{\left|\langle\text{emission}\rangle\right|^2}{\left|\langle\text{absorption}\rangle\right|^2} = \frac{n+1}{n}\,, \tag{40}$$

so emission is slightly more probable.

In the interaction Hamiltonian we need to consider the actual shapes of the orbitals of the atoms: it is a difficult search.

1.1 A crash course in LASER

For this part, see the Saleh-Teich.

Let us say we have two states with energies $E_{1,2}$ with $E_2 - E_1 = \hbar\omega$. We can either have emission, absorption or stimulated emission, as we were discussing.

The dipole term is approximately constant. The probability density of thhe deexcitation is given by

$$w_i = \frac{\overline{n}}{t_{\text{sp}}}\,, \tag{41}$$

where t_{sp} is such that $\mathbb{P} = 1/t_{sp}$.

What? what are the units here?

We'd like to have amplification of the emission between the states 2 and 1: however the emission is always more likely than the absorption, asymptotically they have the same probability.

The way to solve this is introducing more states: the easy way to do it is to introduce two of them, call them 0 and 3, one below and one above our 1 and 2. These are still excitation states of a certain atom.

The *pumping* is the temporal and spatial density of the $0 \to 3$ transitions, then the state descends through 2, 1, and finally 0.

We need to choose the atom appropriately, with a good probability of the atom absorbing the pumping, and a high probability of doing $3 \to 2$. The $2 \to 1$ transition must have a reasonably low probability. Neodymium is a good candidate. For it, the characteristic time of state 2 is of the order of the hundreds of µs.

Recall the law of Boltzmann statistics:

$$\frac{N_2}{N_1} = \exp\left(-\frac{E_2 - E_1}{k_B T}\right). \tag{42}$$

The construction we made creates an *inversion* of this population: the population of state 2 becomes larger than that of state 1.

We are interested in $N = N_2 - N_1$: in the thermodynamical equilibrium case this is almost $-N_1$ since N_2 is negligible. In our case, instead, it becomes $N = Wt_{sp}$.

It is useful to introduce the concept of *optical gain*: let's say we have a cavity of length d, then the frequency corresponding to the lowest mode is $\nu_f = c/2d$ and we can consider modes like $\nu = q\nu_f$.

The number flux is

$$\Phi = \frac{I}{h\nu}, \tag{43}$$

where I is the light intensity; we are interested in $\mathrm{d}\Phi/\mathrm{d}z$, where z is the coordinate along our cavity. It will look like:

$$\frac{\mathrm{d}\Phi}{\mathrm{d}z} = \gamma(\nu)\Phi(z), \tag{44}$$

where $\gamma = N\sigma(\nu)$, N being the one from above, $N_2 - N_1$. If this is positive, then we have optical gain.

We want our laser to create a *ray* of light: this is not trivial, the simplest thing is to create a cavity where one of the mirrors actually has a non-1 reflectivity, so that a certain portion of light escapes.

This can be summarized with the average permanence time of a photon in the cavity: if the intensity in terms of the position looks like $I(z) = I_0 \exp(-\alpha_r z)$ for some coefficient α_r, then we can also write $\alpha_r = 1/c\tau$, where we introduced the characteristic time τ.

The rule will then be $\gamma > \alpha_r$: if this is the case, then the radiation is amplified more than it gets out. If this is not the case, we basically have a thermal source.

Fri Jan 17 2020

Dialogue: "take a photon".

Nonlinear crystals: in general the formula for the polarization vector in terms of the electric field looks like

$$P_i = \chi^{(1)}_{ij} E_j + \chi^{(2)}_{ijk} E_j E_k + \dots , \tag{45}$$

with $\chi^{(m)}$ being the m-th order susceptibility tensor: the linear susceptibility is what the basic index of refraction is based on, but the higher order interactions allow for interesting effects.

For example, green laser pointer start off with an infrared light, and then cuts the frequency in half.

An atom is ionized, the free electron is accelerated by the light's electric field (thus, it absorbs photons), and then it is reabsorbed.

This practically allows for up-conversion of low-frequency light.

Typo in formula D4: the $E^{(+)}$ is the one with the creation operator.

The photon going straight is the "pump" photon, the other two nonlinear photons are the "idler" and "signal".

Typical rates of production: 10^{-7} to 10^{-11}.

The process is called *Spontaneous Parametric Down-Conversion*.

In type-1 SPDC we have the same polarization, and a cone is emitted. In type-2 SPDC they have orthogonal polarizations: then they perceive different susceptibility tensors, and two different cones of light are emitted. The intersection of the two cones are those in which we have polarization entangled light.

With some weird second-quantization notation we can write the Bell state

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|H\rangle_s |V\rangle_i + |V\rangle_s |H\rangle_i \right) , \tag{46}$$

where s and i denote signal and idler, while H and V denote horizontal and vertical polarizations.

Schrödinger: unlike the classical case, knowledge of a full system does *not* come from the knowledge of all its parts.

What is the quantum mechanical description of a beam splitter? It does *not* work to multiply the transmission and reflection coefficients by annihilation operators. The actual operatorial description must describe all of the four sides of the BS: we will have a

$$\begin{bmatrix} \hat{a}_2 \\ \hat{a}_3 \end{bmatrix} = M \begin{bmatrix} \hat{a}_0 \\ \hat{a}_1 \end{bmatrix} , \tag{47}$$

with M being a unitary matrix:

$$M = \exp\left(i \frac{\pi}{4} \left(\hat{a}_0^\dagger \hat{a}_1 + \hat{a}_0 \hat{a}_1^\dagger \right) \right) , \tag{48}$$

so the process is coherent. So, if we send a state $|01\rangle$ (in the Hilbert space of photons going right, down before the BS) to the BS it returns

$$\frac{1}{\sqrt{2}}(i\,|10\rangle + |01\rangle) \tag{49}$$

in the space of photons going right, down after the BS. For coherent states we have

$$|0\alpha\rangle \to \left|i\frac{\alpha}{\sqrt{2}}\right\rangle \otimes \left|\frac{\alpha}{\sqrt{2}}\right\rangle , \tag{50}$$

so there is no entanglement. If we send in two photons, one from up and one from the left, we will always find two photons coming out to the right or downwards. The non-interactions between the photons and the BS destructively interfere.

The photons must arrive "at the same time" for this: the time difference must be small compared to the coherence time of the beam, the time before which the waves have a *phase jump*.

$$R_{\text{coincidences}} = 1 - \exp\Big(-(\Delta\omega)^2(t-t_0)^2\Big) , \tag{51}$$

an inverse Gaussian: $\Delta\omega$ is the *bandwidth* and it gives the inverse of the std of the gaussian.

Monday 2020-3-16, compiled May 12, 2020

2 Vallone's part

We will discuss some protocols with which to generate entanglement, how it is measured and how it is used.

Then, we would have another lab activity in which we are shown how to make a Quantum Key Distribution protocol.

Last time (?) we discussed the Ambu-Mandel effect: this is about the fact that two photons impacting on a beam splitter can either go both up or both down.

What happens if the two impacting photons are entangled? Let us denote a and b as the incoming photons, while c and d are the ones coming out.

Let us assume these two photons start out as a singlet in their polarization:

$$\left|\psi^-\right\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_A\,|V\rangle_B - |V\rangle_A\,|H\rangle_B\right) \tag{52}$$

$$= \frac{1}{\sqrt{2}}\left(a_H^\dagger b_B^\dagger - a_V^\dagger b_H^\dagger\right)|0\rangle , \tag{53}$$

where the second expression is the same as the first, written in the second quantization formalism. The operators can be written as

$$a^\dagger = \frac{1}{\sqrt{2}}\left(c^\dagger + id^\dagger\right) \tag{54}$$

$$b^\dagger = \frac{1}{\sqrt{2}}\left(d^\dagger + ic^\dagger\right) , \tag{55}$$

which means that when the photon changes direction it picks up a phase delay of $i = e^{i\pi/2}$.

Substituting this in, we find

$$\left|\psi^-\right\rangle = \frac{1}{\sqrt{2}^3}\left[\left(c_H^\dagger + id_H^\dagger\right)\left(d_V^\dagger + ic_V^\dagger\right) - \left(c_V^\dagger + id_V^\dagger\right)\left(d_H^\dagger + ic_V^\dagger\right)\right]|0\rangle \tag{56}$$

$$= \frac{1}{\sqrt{2}}\left[c_H^\dagger d_V^\dagger - c_V^\dagger d_H^\dagger\right]|0\rangle\ , \tag{57}$$

since these operators commute if they act on different spaces. So, the photons must always come out in different directions. We can compute this for different Bell states:

$$\left|\psi^\pm\right\rangle = \frac{1}{\sqrt{2}}\left[a_H^\dagger b_V^\dagger \pm a_V^\dagger b_H^\dagger\right]|0\rangle \tag{58}$$

$$\left|\phi^\pm\right\rangle = \frac{1}{\sqrt{2}}\left[a_H^\dagger b_H^\dagger \pm a_V^\dagger b_V^\dagger\right]|0\rangle\ , \tag{59}$$

and with similar steps as before we get that for the $\psi^\pm$ states (singlet) the photons come out in different states, while for the $\phi^\pm$ (triplet) states they come out the same side.

This is idealized, as if the photons had an infinite wavelength. In the lab, we can plot the number of coincidences as the delay in time of arrival changes: the coincidences have a bump or a hump for $\Delta t = 0$; for the singlets the coincidences go to zero, while the triplets the coincidences double from the regular (non-entangled) case.

We can have a projective measurement in our space to be one which distinguishes these 4 states: this is a Bell State Measurement.

We can check whether we see ψ or ϕ by looking at coincidence or no coincidence, and by looking at whether the polarizations are the same or different we can see whether we have the $+$ or $-$ in $\psi^\pm$ (or $\phi^\pm$ respectively).

2.1 Quantum Teleportation

This means transferring the wavefunction from a particle to another. Particles are indistinguishable, the only thing which is different from one to the other is the wavefunction. So, if we can transfer the wavefunction we have transferred the particles for any purpose.

"Classical FAX becomes quantum teleportation".

Let us discuss the teleportation protocol. For another reference, see the notes for the course on Quantum Information [Tis19]. The photon starts out with a wavefunction

$$\left|\varphi\right\rangle_A = \alpha\left|0\right\rangle + \beta\left|1\right\rangle\ , \tag{60}$$

and we have an EPR state, with two particles entangled, let us say, in the singlet state $\left|\psi^-\right\rangle$ on particles B and C.

What we should do is a Bell State Measure on particles A and B. Our result has 4 possible outcomes, we codify it into 2 classical bits.

Then, we will apply a unitary transformation depending on these 2 bits on particle C. Then, the state of particle A will be replicated on particle C.

This destroys the state of particle A. This also does not give us any information on the state, or on the parameters α and β. We cannot teleport faster than light, since we are bound to transmitting classical bits.

The state will be

$$|\chi\rangle = |\phi\rangle_A \left|\psi^-\right\rangle_{BC} = (\alpha |0\rangle_A + \beta |1\rangle_A) \otimes \frac{1}{\sqrt{2}}(|01\rangle_{BC} - |10\rangle_{BC}) \tag{61}$$

$$= \frac{1}{\sqrt{2}}(\alpha |001\rangle + \beta |101\rangle - \alpha |010\rangle - \beta |110\rangle), \tag{62}$$

so if we compute

$$_{BC}\left\langle \psi^{\pm}\middle|\chi\right\rangle_{ABC} = \frac{1}{2}(\pm\beta |1\rangle_C - \alpha |0\rangle_C) \tag{63}$$

$$= -\frac{1}{2}(\alpha |0\rangle_C \mp \beta |1\rangle_C), \tag{64}$$

so if we measure ψ^-_{AB} we have $\frac{1}{2}|\varphi\rangle_C$, while if we measure ψ^+_{AB} we will have $\frac{1}{2}\sigma_z |\varphi\rangle_C$.

On the other hand, if we measure $\phi^{\pm}_{AB}$ we will have either $\frac{1}{2}\sigma_x |\varphi\rangle_C$ or $\frac{1}{2}\sigma_y |\varphi\rangle_C$.

The $\frac{1}{2}$ factor accounts for the normalization of the probabilities of obtaining the various states: regardless of $|\varphi\rangle$, we have probability $\frac{1}{4} = \frac{1}{2^2}$ for each of the 4 states. The two classical bits contain no information about the state.

If we do not transmit the two classical bits, the state on particle C becomes completely mixed:

$$\frac{1}{4}|\varphi\rangle\langle\varphi| + \frac{1}{4}\sigma_x |\varphi\rangle\langle\varphi| \sigma_x + \frac{1}{4}\sigma_y |\varphi\rangle\langle\varphi| \sigma_y + \frac{1}{4}\sigma_z |\varphi\rangle\langle\varphi| \sigma_z = \frac{1}{2}\mathbb{1}. \tag{65}$$

If we start with two entangled photons A and B, and clone photon B into photon D, then photons A and D will be entangled. This is *entanglement swapping*. It works because $A's$ wavefunction factors out of everything.

This means that we can have entangled particles even if they have never directly interacted.

This is especially useful if we want to entangle slow, massive particles. In the future, it might be the basis for the *quantum internet*.

This cannot be done if we do not transmit classical information.

2.2 Dense Coding

If we just have one qubit, we can use it to encode only one bit of information.

However, if we use additional entangled qubits we can do better, still by sending just one qubit physically.

Alice and Bob start out with a singlet state $\propto (|01\rangle - |10\rangle)$. Alice applies one of $\mathbb{1}$, σ_x, σ_y or σ_z based on the values of her two classical bits.

The state becomes

$$\mathbb{1} \to \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \left|\psi^-\right\rangle \tag{66}$$

$$\sigma_x \to \frac{1}{\sqrt{2}}(|11\rangle - |00\rangle) = \left|\phi^-\right\rangle \tag{67}$$

$$\sigma_y \to \frac{1}{\sqrt{2}}(|11\rangle - i\,|00\rangle) = \left|\phi^+\right\rangle \tag{68}$$

$$\sigma_z \to \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \left|\psi^+\right\rangle\,, \tag{69}$$

so in the end Alice can measure qubit A, which is sent to her, and qubit B, which she already had. Based on the results of her measurements, she can determine what the two classical bits were.

2.3 Tomography

How do we measure α and β for

$$\left|\psi\right\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,? \tag{70}$$

We can measure along the regular basis to find $|\alpha|^2$ and $\left|\beta\right|^2$. In order to get information about their phases, we apply a Hadamard gate: if we measure along

$$\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) \tag{71}$$

then we find information about $\left|\alpha + \beta\right|^2/2$ and $\left|\alpha - \beta\right|^2/2$.

We can decompose a density matrix ρ as $\rho = r_\mu \Gamma^\mu$, where the Γ^μ are a basis of Hermitian matrices.

Then, if we have a basis $\left|\psi_\alpha\right\rangle$ we can do

$$\mathbb{P}_\alpha = \left\langle\rho\middle|\psi_\alpha\middle|\rho\right\rangle = \sum_\mu r_\mu \left\langle\Gamma^\mu\middle|\psi_\alpha\middle|\Gamma^\mu\right\rangle = \sum_\mu r_\mu B_{\mu\alpha}\,, \tag{72}$$

and this system is solvable as long as the projectors $\left|\psi_\alpha\right\rangle\!\left\langle\psi_\alpha\right|$ are linearly independent (which implies that the matrix $B_{\mu\alpha}$ is invertible).

It is a fact that for a d-dimensional Hilbert space we need $d^2 - 1$ of these.

For a qubit, we can write its density matrix as

$$\rho = \frac{1}{2}(\mathbb{1} + \vec{r}\cdot\vec{\sigma})\,; \tag{73}$$

in this case the four states needed are $P_0 = |0\rangle\langle 0|$, $P_1 = |1\rangle\langle 1|$, $P_+ = |+\rangle\langle +|$, $P_- = |-\rangle\langle -|$. These are not independent as states, however they are independent as projectors.

Then, we can recover the components of the Bloch vector representation as

$$r_z = P_0 - P_1 \tag{74}$$

$$r_x = 2P_+ - 1 \tag{75}$$

$$r_y = 2P_1 - 1\,, \tag{76}$$

so in general the only way to recover all the information about a quantum state is to project it along linearly independent projectors (or, really, the necessity is that the projectors span the whole Hilbert space).

Today we will discuss another application of entanglement: Quantum Key Distribution. For more details, see [Sca+09].

Friday 2020-3-20, compiled May 12, 2020

3 Quantum Key Distribution

The idea is that it is possible to exchange two keys between two people, in an *unconditional* way, as opposed to the current way of doing security, which is based on hard-to-solve problems.

If Alice and Bob have a shared key K, they can use a *one-time-pad* to communicate.

Say X is our message: then Alice constructs $Y = X \oplus K$, which is completely random since K is.

When Bob receives the message, he does $Y \oplus K = X \oplus K \oplus K = X$. This is old classical cryptography, it was discovered by Shannon.

This works as long as K is indeed *one-time*: if it is reused, an attacker can start reconstructing the message: otherwise, .

So, the QKD is about transmitting the key. The most famous protocol to do this is BB84. Most of the things which will be covered today are covered in Rev Mod Phys 81, 1301 (2009).

The basis of the algorithm is a public quantum channel between Alice and Bob. The thing which is needed is for the channel to be *verified*, so that Alice is sure to be talking to Bob. Eve can be watching the passing qubits.

Alice can prepare four possible states, which she associates to two logical bits: $|0\rangle$ and $|+\rangle$ are associated with 0, while $|1\rangle$ and $|-\rangle$ are associated with 1.

Bob either measures σ_z or σ_x. It they use the same basis, Bob measures the same thing Alice sent.

If they use a different basis, then the result is random, since $\left|\langle \pm|0\rangle\right|^2 = \left|\langle \pm|1\rangle\right| = 1/2$.

So, there is a need to do *sifting* later: after the transmission, Alice and Bob say publicly which bases they used. With this information, they discard the qubits for which they used different bases.

Any measurement by the eavesdropper necessarily increases the Q-Bit Error Rate, which can be detected by Alice and Bob.

If Eve performs an "Intercept and Resend" attack, $1/2$ of the time she will get the basis wrong, and those times she will create an error half of the time. So, in this case we will have a QBER equal to 25 %.

This can be measured by selecting, a posteriori, some qubits to be used as a check.

Alice could also use the states $|+i\rangle$ and $|-i\rangle$, which are eigenstates of σ_y. Using these states we can increase the security.

The probabilities can be changed: we can have probabilities ϵ for σ_x and σ_y, while we use $1 - 2\epsilon$ probability for σ_z.

Then, we encode the key using only σ_z, so we are communicating $\approx 1 - 4\epsilon$ of the time. We use the qubits encoded with σ_x and σ_y to measure how many times Eve has been

measuring, since she will be always measuring σ_z.

Eve cannot determine which basis is being used by Alice, since the mixed states corresponding to having $|0\rangle$ or $|1\rangle$ with equal probability and to having $|+\rangle$ or $|-\rangle$ with equal probability are the same, $\rho = \frac{1}{2}\mathbb{1}$.

This works well if the devices are working as expected. If the implementation is insecure, QKD can still be breached: so, we want to get *device-independent* implementations.

A possible implementation is one in which we use an entangled source which gives us pairs with $\left|\Psi^-\right\rangle$.

Then, Alice measures σ_x and σ_z and so does Bob. Using the correlations between Alice and Bob we can determine whether the qubits are being generated entangled or not. The state is

$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle)\,, \tag{77}$$

so the measurements are precisely anticorrelated for both bases 01 and +-.

So, we can do QKD with black boxes. However, this is difficult to implement.

The receiver is more vulnerable to attacks, since they can receive any signal from the outside. So, we want to do *measurement device independent* coding: Alice and Bob each prepare the four states with equal probabilities, they send it to an untrusted station C, in which there is a beamsplitter. This performs a Bell measurement: if C sees a coincidence, then they communicate this to A and B: this means that the measured state is $\left|\Psi^-\right\rangle$. This means that the original qubits were opposite, but there is no information as to what the states originally were.

If the operator at C does anything else other than the Bell measurement, this can be detected by Alice and Bob by looking at the QBER.

By adding some more detectors we can also measure $\left|\Psi^+\right\rangle$; then we do efficient BB84 by mostly sending in one basis. This way, we can also get an efficiency of $1-\epsilon$.

Now, how do we measure the secret Key Rate? It is defined by

$$r = I_{AB} - I_E\,, \tag{78}$$

where I_{AB} is the mutual information of Alice and Bob, while I_E is the information of the Eavesdropper.

The definition of I_{AB} is:

$$I_{AB} = H(A) - H(A|B)\,, \tag{79}$$

where $H(A)$ is the Shannon entropy of Alice:

$$H(A) = -\sum_{x=0,1} p_x \log_2 p_x\,. \tag{80}$$

If the bits are random, then $H(A) = 1$. On the other hand,

$$H(A|B) = -\sum_{\substack{a=0,1\\b=0,1}} p_{ab} \log_2 p_{a|b}\,, \tag{81}$$

which is zero if Alice and Bob's bits are perfectly correlated. It can be shown that

$$H(A|B) = h_2(Q) = -Q\log_2 Q - (1-Q)\log_2(1-Q)\,, \tag{82}$$

where Q is the error rate.

So, we write this as $I_{AB} = 1 - h_2(Q)$. Q is the number of bits which are wrong, and the formula tells us that in order to correct these errors we need to reveal $h_2(Q)$.

It can be shown that the information of the eavesdropper in the BB84 case is

$$I_E = h_2(Q)\,. \tag{83}$$

With the 6-state coding we have

$$I_E = Q + (1-Q)h_2\left(\frac{1-3Q/2}{1-Q}\right). \tag{84}$$

This is purely quantum: classically there is no connection between I_E and Q. So, for BB84 the error rate must be $Q \leq 11\,\%$.

So, we need to do *error correction* and then *privacy amplification* so that the eavesdropper has no residual information. Privacy amplification reduces the key length by a factor $1/r$, so we get bits which are surely secure.

What we do, practically, is to use an attenuated laser. The state of the laser is a coherent one:

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_n \frac{\alpha^n}{\sqrt{n!}}\,|k\rangle\ . \tag{85}$$

We can attenuate the laser so that we have $|\alpha| = \mu$, with $\mu = 1$: usually we will have zero photons, often one, but sometimes 2: this is an issue, since the attacker can take one and leave the other: this is called Photon Number Splitting.

What can be done is to use a *decoy state*: we use three values for the intensity, $\mu = 1$, but also $\nu_1 = .1$ and $\nu_2 = 0$. Using this, we can see whether there is a PNS attack or not.

So, from the source point of view we have no issue in using a classical source like a laser.

We can always decompose a Hermitian matrix in a basis: if $M = M^\dagger$ then $M = r_\mu \hat{\Gamma}_\mu$. If we choose the matrices so that $\mathrm{Tr}\left[\hat{\Gamma}_\mu \hat{\Gamma}_\nu\right] = \delta_{\mu\nu}$, we can use the Euclidean scalar product.

Friday 2020-3-27, compiled May 12, 2020

4 Bell nonlocality

We will follow some of [Bru+14].

When first encountering QM, people usually think in terms of statistics.

Let us make an explicit example for a hidden variable theory.

Let us suppose we have a qubit which is described by the density matrix

$$\rho = \frac{1}{2}(\mathbb{1} + \vec{s}\cdot\vec{\sigma})\,, \tag{86}$$

where $\vec{s}$ is a unit vector in the Bloch sphere. Now, we can measure spins: our observables are in the form $\hat{A} = \vec{a} \cdot \vec{\sigma}$, which means we are measuring the spin in the direction of the unit vector $\vec{a}$.

The expectation value is

$$\left\langle \hat{A} \right\rangle = \mathrm{Tr}\Big(\hat{A}\rho\Big) = \vec{a} \cdot \vec{s} = \cos\theta = (+1)\mathbb{P}(+1) + (-1)\mathbb{P}(-1)\,, \tag{87}$$

where θ is the angle between $\vec{a}$ and $\vec{s}$.

Is the output of the measurement prescribed by some hidden variable λ?

If so, we would need to describe the state with the pair (ρ, λ). Then, if $A(\lambda)$ is the function associating a value of λ to its outcome we will have

$$\left\langle \hat{A} \right\rangle = \int \mathrm{d}\mu_\rho(\lambda)\, A(\lambda)\,. \tag{88}$$

In principle $A(\lambda)$ would also depend on ρ, but we can rescale the measure on the space so that it doesn't.

Suppose $\vec{\lambda}$ is defined on the hemisphere $\vec{\lambda} \cdot \vec{s} \geq 0$ and $\left|\vec{\lambda}\right| = 1$. Then, $\mathrm{d}\mu_\rho(\lambda)$ is a uniform density function defined there, and it is zero otherwise.

Let us define the unit vector $\vec{a}'$ so that

$$A(\lambda) = \mathrm{sign}(\vec{\lambda} \cdot \vec{a}')\,, \tag{89}$$

and so that $\vec{a}'$ is in the plane defined by $\vec{s}$ and $\vec{a}$ and the angle between $\vec{s}$ and $\vec{a}'$ is θ', defined by

$$1 - \frac{2\theta'}{\pi} = \cos\theta\,. \tag{90}$$

With this, we have a statistical model which describes quantum mechanics.

The problem comes along when we consider Bell inequalities, which deal with multiple systems.

Then, in the Hidden Variable theory we will have

$$\left\langle \hat{A} \otimes \hat{B} \right\rangle = \int \mathrm{d}\mu_\rho(\lambda)\, F(\lambda)\,, \tag{91}$$

but if we assume we have locality then (as shown in Phys Rev 47, 777 (1935), the EPR paper) we must impose that there can be no causal link between events which are spacelike-separated. So, under a Local Hidden Variable model we must have that the events are independent: so we must write

$$\left\langle \hat{A} \otimes \hat{B} \right\rangle = \int \mathrm{d}\mu_\rho(\lambda)\, A(\lambda)B(\lambda)\,. \tag{92}$$

Reality means determinism: if we have reality and we fix λ then the result of the measurement is also fixed.

What Bell did was to probe that this kind of expression is incompatible with the prediction of QM: if we consider the operator

$$S = \left\langle \hat{A} \otimes \hat{B} \right\rangle + \left\langle \hat{A} \otimes \hat{B}' \right\rangle + \left\langle \hat{A}' \otimes \hat{B} \right\rangle - \left\langle \hat{A}' \otimes \hat{B}' \right\rangle , \tag{93}$$

where $\hat{A}'$ and $\hat{B}'$ are two different observables Alice and Bob can choose to measure randomly, and which both have eigenvalues ± 1. Then, we have that its expectation value is

$$\int \mathrm{d}\mu(\lambda) \left[A(B + B') + A'(B - B') \right] , \tag{94}$$

and this is upper-bounded by 2. If we do an experiment, and measure a value which is greater than 2, then we have falsified LHV theory. Quantum Mechanics tells us we can indeed go beyond 2. If we choose $\vec{a}$ and $\vec{a}'$ at right angles to each other, $\vec{b}$ and $\vec{b}'$ likewise, with an angle of $\pi/4$ between them, then it can be shown that if the state ρ is a singlet then

$$\left\langle (\vec{a} \cdot \vec{\sigma}) \otimes (\vec{a} \cdot \vec{\sigma}) \right\rangle = -\vec{a} \cdot \vec{b} , \tag{95}$$

so if $\vec{a} = \vec{b}$ we have perfect anticorrelation. So we get

$$\left\langle |S| \right\rangle = \left| -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} \right| = 2\sqrt{2} \approx 2.8 > 2 . \tag{96}$$

So, we either reject determinism or we reject locality.

In the orthodox interpretation of QM the theory is simply nondeterministic.

This is wonderful theoretically, but there are loopholes. Only in 2015 the experiment was done in a loophole-free way.

4.1 Loopholes

4.1.1 Freedom of choice

In the experiment we discussed before Alice and Bob could choose in a random way between the two measurements. This is important since if the measurements are predetermined then that is a hidden variable. If the measurements are fixed then we can describe the statistics with a hidden variable theory.

4.1.2 Locality

The choice of the measurement basis must be done late enough so that the events are still spacelike separated. So, we should choose the measurement basis so that the photons have almost arrived when we decide.

4.1.3 Detection loophole

Photons are not revealed efficiently: they are lost in detection, so we may reveal only a small fraction of the total photons.

4.1.4 Superdeterminism

It has not been possible yet to exclude that all of nature is completely predetermined.

When we write the correlation between two operators, we write something like

$$\langle A \otimes B \rangle = \sum_{ij} ij \mathbb{P}_{AB}(ij)\,, \tag{97}$$

but we have that $\mathbb{P}(a,b) + \mathbb{P}(\overline{a},b) = \mathbb{P}(b)$. Then, we can find that

$$\langle A \otimes B \rangle = 4\mathbb{P}(a,b) - 2P_A(a) - 2P_B(b) + 1\,, \tag{98}$$

which is useful since it contains only positive results. This allows us to write

$$S_{CHSH} = 4S_{CH} + 2 \qquad \text{where} \qquad S_{CH} = \mathbb{P}(a,b) + \mathbb{P}(a',b) + \mathbb{P}(a,b') - \mathbb{P}(a) - \mathbb{P}(b)\,, \tag{99}$$

and $S_{CHSH} \leq 2$ is equivalent to $S_{CH} \leq 0$. The advantage is that we do not need to normalize for the total number of events: we can write this directly as

$$N(a,b) + N(a',b) + N(a,b') - N(a) - N(b) \leq 0\,, \tag{100}$$

so we have no issue with lost photons.

If the efficiency is η for each channel, then experimentally we will measure

$$S_{CH}^{\text{exp}} = \eta^2 \left[\mathbb{P}(a,b) + \mathbb{P}(a',b) + \mathbb{P}(a,b')\right] - \eta\left[\mathbb{P}(a) + \mathbb{P}(b)\right], \tag{101}$$

where the term multiplying η^2 is precisely $S_{CHSH} + \mathbb{P}(a) + \mathbb{P}(b)$. If we want to violate the inequalities, we must have $S_{CH}^{\text{exp}} > 0$: the minimum efficiency is

$$\eta_* = \frac{\mathbb{P}_A(a) + \mathbb{P}_B(b)}{S_{CH}^{Q} + P_A(a) + P_B(b)}\,, \tag{102}$$

and if we use maximally entangled singlet states we have $\eta_* \approx 2\left(\sqrt{2} - 1\right) \approx 83\,\%$.

This is combined efficiency: an emitted photon must have a $\geq 83\,\%$ probability of being revealed.

The detectors used had less efficiency than this: actually, if we have a state like $\cos\theta\,|00\rangle + \sin\theta\,|11\rangle$ we have a lower η_*: the best thing is in the limit of $\theta \to 0$, so we will need $\eta_* \approx 2/3 \approx 67\,\%$.

If we do not have this efficiency, we must make a *fair sampling assumption*: the photons we do measure are a representative sample of all the photons.

There were three works published in 2015 which did this:

1. Nature 526, 682
2. PRL 115, 250401
3. PRL 115, 250402

In the works in PRL they used photons, while the work in Nature used electron spins, entangling them with entanglement swapping. The experiment using electrons did not have the detection loophole, but they are very much subject to the locality loophole.

We can further extend Bell inequalities in multipartite systems.

If we have three systems, we can measure (denoting $\sigma_x = X$ and so on)

$$M_1 = X_a X_b X_c \tag{103}$$
$$M_2 = -Y_a Y_b X_c \tag{104}$$
$$M_3 = -Y_a X_b Y_c \tag{105}$$
$$M_4 = -Y_a Y_b Y_c \,, \tag{106}$$

and one can see that $M_1 M_2 M_3 = -M_4$, so classically if we assume we can write the expectation value as

$$\int \mathrm{d}\mu \, A(\lambda) B(\lambda) C(\lambda) \,, \tag{107}$$

and we can violate these with the GHZ state:

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle) \,, \tag{108}$$

and we can see that

$$\langle M_i \rangle = +1 \,, \tag{109}$$

for each of these. We can write this as an inequality with $M_1 + M_2 + M_3 + M_4 \leq 2$.

The nice thing is that we can do this with perfect correlations, while in CHSH we do not have perfect correlations.

One could actually see that this can be generalized to N qubits: as we increase the dimension, the violation increases exponentially:

$$\frac{\beta_Q}{\beta_c} \sim 2^N \,, \tag{110}$$

where β is the value we obtain for the inequality.

No one has yet done a loophole-free measurement with three subsystems, but loophole-wrought measurements have indeed been done.

We can also improve the violation s increasing the dimensionality of two systems, that is, using Q-dits.

Often "quantum nonlocality" is discussed, but this is imprecise: we cannot really prove that quantum mechanics is nonlocal, we can only say that it either is nonlocal or nondeterministic.

Why is it important to choose the measurements randomly? If we already know what the measurement bases will be, then we can create a hidden variable model which will give the correct results.

Friday 2020-4-3, compiled May 12, 2020

5 Continuous variables in QM

If we have a single mode, then we have

$$a^\dagger_{\lambda,\epsilon,\vec{k}} \stackrel{\text{def}}{=} a^\dagger \qquad \text{where} \qquad \left[a, a^\dagger\right] = 1\,, \tag{111}$$

with which we can generate n-photon states as

$$|n\rangle = \frac{\left(a^\dagger\right)^n}{\sqrt{n!}}\,|0\rangle\ , \tag{112}$$

where our Hilbert space must be infinite-dimensional since we can have as many photons as we want.

So, we can define

$$a = \hat{X}_1 + i\hat{X}_2\,, \tag{113}$$

where we have

$$\left[\hat{X}_1, \hat{X}_2\right] = \frac{i}{2}\,, \tag{114}$$

so this real-imaginary decomposition is like a position-momentum decomposition. These operators are called *quadratures*, they are self-adjoint.

We are in second quantization, so the wavefunction is written as

$$|\psi\rangle = \int \mathrm{d}^3k \int \mathrm{d}\lambda \sum_\epsilon a^\dagger_{\lambda,\epsilon,\vec{k}}\,|0\rangle\ . \tag{115}$$

5.1 P-function

Any state can be written as

$$\rho = \sum_{n,m} \rho_{n,m}\,|n\rangle\langle m|\ , \tag{116}$$

since the single-particle states are a basis. If we write a coherent state

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_n \frac{(a^\dagger)^n}{n!}\,|0\rangle\ , \tag{117}$$

we can use the expression

$$\int \frac{\mathrm{d}^2\alpha}{\pi}\,|\alpha\rangle\langle\alpha| = \mathbb{1}\,, \tag{118}$$

which allows us to write

$$\rho = \frac{1}{\pi}\int \mathrm{d}^2\alpha\, P(\alpha)\,|\alpha\rangle\langle\alpha|\ . \tag{119}$$

Note that we have $|\alpha\rangle\langle\alpha|$, not $|\alpha\rangle\langle\beta|$. This can be done since the coherent states are not linearly independent, they are an overcomplete basis.

This must be normalized, so that

$$\int \mathrm{d}^2\alpha \, P(\alpha) = 1 \,. \tag{120}$$

If this $P(\alpha)$ was always positive, then we would have classical states, a statistical mixture.

The over-completeness relation is found by expanding the integral

$$\langle n| \left[\int \frac{\mathrm{d}^2\alpha}{\pi} \, |\alpha\rangle\langle\alpha| \right] |m\rangle = \delta_{nm} \,. \tag{121}$$

5.2 Husini-function

Given the P-function, we have

$$\hat{O} = \int \frac{\mathrm{d}^2\alpha}{\pi} P_O(\alpha) \, |\alpha\rangle\langle\alpha| \tag{122}$$

for any operator $\hat{O}$, so we will have

$$\left\langle \hat{O} \right\rangle_\rho = \mathrm{Tr}\left(\hat{O}\rho\right) \int \frac{\mathrm{d}^2\alpha}{\pi} P_O(\alpha) \, \langle\alpha|\rho|\alpha\rangle \,, \tag{123}$$

so we define

$$\frac{1}{\pi} \, \langle\alpha|\rho|\alpha\rangle = Q(\alpha) \,, \tag{124}$$

which is called the Husini function.

The generating function $C(k)$ of a pdf $p(x)$ is defined as

$$C(x) = \int e^{ikx} p(x) \, \mathrm{d}x \,, \tag{125}$$

so we will have

$$\left. \frac{\mathrm{d}^n C(k)}{\mathrm{d}x^n} \right|_{k=0} = i^n \left\langle x^n \right\rangle_p \,. \tag{126}$$

We can do a similar thing in the quantum realm. We can define

$$\chi(\eta) = \mathrm{Tr}\left[\rho \underbrace{\exp\left(\eta\hat{a}^\dagger - \eta^*\hat{a}\right)}_{D(\eta)} \right] , \tag{127}$$

which is somewhat like a Fourier transform. The operator $D(\eta)$ is called the displacement operator: its action is

$$D(\alpha) \, |0\rangle = |\alpha\rangle \,, \tag{128}$$

so it generates the coherent states. In phase space, it translates from the vacuum to the coherent state $|\alpha\rangle$. We can write it as

$$D(\alpha) = \exp\left(\alpha a^\dagger - \alpha^* a\right) = \exp\left(-\frac{|\alpha|^2}{2}\right)\exp\left(\alpha a^\dagger\right)\exp(-\alpha^* a)\,, \tag{129}$$

but $e^{-\alpha^* a}\,|0\rangle = |0\rangle$, since $a\,|0\rangle = 0$.

We also define the operators

$$\chi_N(\eta) = \mathrm{Tr}\left[\rho e^{\eta a^\dagger} e^{-\eta^* a}\right] \qquad \text{and} \qquad \chi_A(\eta) = \mathrm{Tr}\left[\rho e^{-\eta^* a} e^{\eta a^\dagger}\right], \tag{130}$$

where the N stands for normal-ordering; these are

$$\chi_N(\eta) = e^{\frac{1}{2}|\eta|^2}\chi(\eta) \qquad \text{and} \qquad \chi_A(\eta) = e^{-\frac{1}{2}|\eta|^2}\chi(\eta)\,. \tag{131}$$

So, with these, we can define

$$P(\alpha) = \frac{1}{\pi}\int \mathrm{d}^2\eta\, e^{\overline{\eta}\alpha - \eta\overline{\alpha}}\chi_N(\eta) \qquad \text{and} \qquad Q(\alpha) = \frac{1}{\pi}\int \mathrm{d}^2\eta\, e^{\overline{\eta}\alpha - \eta\overline{\alpha}}\chi_A(\eta)\,, \tag{132}$$

while

$$W(\alpha) = \frac{1}{\pi}\int \mathrm{d}^2\eta\, e^{\overline{\eta}\alpha - \eta\overline{\alpha}}\chi(\eta)\,, \tag{133}$$

the latter being the Wigner function. These are all equivalent, we can use whichever is more convenient, which usually is the Wigner function.

Similarly to the classical case, we have

$$\left\langle a^{\dagger m} a^n \right\rangle_\rho = \frac{\partial^n}{\partial\eta^n}\frac{\partial^m}{\partial\overline{\eta}^m}\chi_N(\eta) \tag{134}$$

$$\left\langle a^n a^{\dagger m} \right\rangle_\rho = \frac{\partial^n}{\partial\overline{\eta}^n}\frac{\partial^m}{\partial\eta^m}\chi_A(\eta) \tag{135}$$

$$\left\langle \left\{a^n, a^{\dagger m}\right\} \right\rangle_\rho = \frac{\partial^n}{\partial\overline{\eta}^n}\frac{\partial^m}{\partial\eta^m}\chi(\eta) \tag{136}$$

$$. \tag{137}$$

For coherent states we have

$$\langle\alpha|a|\alpha\rangle = \alpha\,, \tag{138}$$

while

$$\left\langle \Delta X_1^2 \middle| \alpha \middle| \Delta X_1^2 \right\rangle = \left\langle \Delta X_2^2 \middle| \alpha \middle| \Delta X_2^2 \right\rangle = \frac{1}{4}\,. \tag{139}$$

The Wigner function of a coherent state is

$$|\beta\rangle \to W(\alpha) = \frac{2}{\pi}e^{-2|\alpha-\beta|^2}\,. \tag{140}$$

Usually we will calculate probability densities like

$$\langle\rho|x_1|\rho\rangle = p(x_1) = \int \mathrm{d}x_2\, W(x_1, x_2)\,. \tag{141}$$

While $W(\alpha)$ can be both negative and positive, its integral along any line in the complex plane will be ≥ 0, since we can define

$$X_\theta = \frac{1}{2}\left(ae^{-i\theta} + a^\dagger e^{+i\theta}\right). \tag{142}$$

In this coherent state, we will have

$$Q(\alpha) = \left|\langle\alpha|\beta\rangle\right|^2 = \frac{1}{\pi}e^{-|\alpha-\beta|^2}\,, \tag{143}$$

while

$$P(\alpha) = \delta(\alpha - \beta)\,. \tag{144}$$

How do we measure these? We need a type of measure called **homodyne detection**.

We have a beamsplitter, on one side we have our state ρ, on the other we have a laser: an almost-classical state $|\beta\rangle$ with $\beta \gg 1$.

Outside the BS we then measure $I_c - I_d$, which is the average on ρ of X_θ, where $\beta = |\beta|e^{i\theta}$.

This is because $c^\dagger = b^\dagger + ia^\dagger$ and $d^\dagger = a^\dagger + ib^\dagger$. So, we are measuring

$$I_c - I_d \propto c^\dagger c - d^\dagger d = 2ia^\dagger b - 2ib^\dagger a\,, \tag{145}$$

but since we need to do this on the state $\rho \otimes |\beta\rangle\langle\beta|$ we get

$$2i\beta\left\langle a^\dagger\right\rangle_\rho - 2i\beta^*\left\langle a\right\rangle_\rho\,, \tag{146}$$

which is precisely

$$2i|\beta|\left\langle\left[ie^{i\theta}a^\dagger - ie^{-i\theta}a\right]\right\rangle_\rho\,, \tag{147}$$

which corresponds to the Wigner function integrated on a line at an angle θ.

This is a macroscopic measurement! We measure bulk currents, however if we measure the variance

$$\left\langle\Delta I_{cd}^2\right\rangle = 4|\beta|^2\left\langle\Delta X_\theta^2\right\rangle_\rho + \mathcal{O}\left(|\beta|\right). \tag{148}$$

The noise here is intrinsically quantum. If $\beta \gg 1$ we can do this approximation.

We can then do a sort of tomography on our state.

A different measurement is called a double homodyne, or heterodyne.

Now our detector is split in two, we use the same laser but in two beam splitters, with a respective phase of $\pi/2$. We are effectively using a POVM

$$\Pi_\beta = \frac{1}{\pi}|\beta\rangle\langle\beta|\,, \tag{149}$$

where

$$\beta = X_1 + iX_2\,. \tag{150}$$

Then we will have $\mathrm{Tr}\Big(\rho\Pi_\beta\Big) = \pi^{-1}\left\langle\rho\middle|\beta\middle|\rho\right\rangle = Q(\beta)$.

In classical communication, this is called a coherent detector.

6 Squeezing

Coherent states are really classical states. We know that

$$\Delta X_1 \Delta X_2 \geq \frac{1}{4} \qquad \text{and} \qquad \left\langle \Delta X_\theta^2 \right\rangle = \frac{1}{4}\forall\theta\,, \tag{151}$$

but this constraint can also be satisfied by "squeezed" states: these have large variances in one direction and small in the other.

These are written using the squeezing operator:

$$S(\xi) = \exp\left(\frac{1}{2}\left(\xi^* a^{\dagger 2} - \xi a^2\right)\right). \tag{152}$$

Since we have the squares of the operators, we have different behaviour from before. We can write S as

$$S(\xi) = \frac{1}{\sqrt{\mu}}\exp\left(-\frac{1}{2}\frac{\nu}{\mu}\alpha^{\dagger 2}\right)\mu^{-a^\dagger a}\exp\left(\frac{1}{2}\frac{\overline{\nu}}{\mu}a^2\right), \tag{153}$$

where

$$\mu = \cosh r, \nu = \sinh re^{i\varphi} \qquad \text{where} \qquad \xi = re^{i\varphi}\,. \tag{154}$$

so we have

$$|\xi\rangle = S(\xi)\,|0\rangle = \frac{1}{\sqrt{\mu}}\exp\left(-\frac{1}{2}\tanh re^{i\varphi}a^{\dagger 2}\right) \tag{155}$$

$$= \frac{1}{\sqrt{\mu}}\sum_n (\dots)\frac{a^{\dagger 2}}{\sqrt{n!}}\,|0\rangle\ , \tag{156}$$

so this state will have only an even number of photons: we will have

$$\sqrt{\left\langle \Delta X_\varphi \right\rangle} = \frac{1}{2}e^{-r} \qquad \text{and} \qquad \sqrt{\langle \Delta X_r\rangle} = \frac{1}{2}e^{+r}\,, \tag{157}$$

so φ tells us along which direction we are squeezing, while r tells us by how much.

This was applied on the vacuum, but then we can do

$$|\xi,\alpha\rangle = D(\alpha)S(\xi)\,|0\rangle\ . \tag{158}$$

This only changes the average, the variances are kept. The operators S and D do not commute.

This can be experimentally generated using nonlinear crystals. The first term in the expansion of $S(\xi)$ is precisely the first term in the spontaneous parametric down-conversion.

The Hamiltonian in SPDC is

$$H = ba^{\dagger 2} - b^\dagger a^2 \,, \tag{159}$$

so we will actually never have an odd number of photons.

Friday 2020-4-10, compiled May 12, 2020

7 Quantum Random Number Generators

Random number: generated by an unpredictable process.

Random numbers are crucial in several applications:

1. information technology and security;
2. scientific simulations;
3. games and lotteries.

Classically, we imagine a coin toss or a dice roll. However, these are deterministic processes: if we know the initial conditions we can determine the outcome.

We have Pseudo RNGs: they are simple and fast, but they have a period, they exhibit non-uniformity, (another thing). (predictability?)

RANDU was used by IBM from the sixties to the nineties.

We start from a seed V_0, and then compute

$$V_{k+1} = 65539 \times V_k \mod 2^{31} \,. \tag{160}$$

This gives us numbers in $[0, 2^{31} - 1]$ which we can normalize to $[0, 1)$.

However there are several flaws in PNRGs.

We can use QRNG: for instance, a diagonal polarization sent through a polarizing beam splitter.

Even if the initial state is perfectly known, the outcome is not predictable.

7.1 Fully trusted QRNG

We have a fully trusted source $|\psi\rangle$, and a fully trusted measurement. The probability of outcome $|z\rangle$ is

$$P_z = \left|\langle z|\psi\rangle\right|^2 . \tag{161}$$

The way to quantify this is the classical min-entropy:

$$H_\infty(Z) = -\max_z \left(\log_2 P_z\right) . \tag{162}$$

The issue is that our starting state may not be pure; instead it is a mixed state, which is pure when considered together with the eavesdropper's state.

It is hard to evaluate the min-entropy in the presence of an eavesdropper.

In general, we will have an entropy source, which is a physical system plus a measurement, from which we extract raw bits, which we then do post-processing to, and finally we read-out the random sequence.

We have three scenarios, with decreasing speed and simplicity, and increasing security:

1. Trusted QRNG;
2. Semi device independent QRNG;
3. Fully device independent QRNG.

7.2 Trusted QRNG

We suppose that the starting state is indeed pure, so the min-entropy is indeed the classical one. We can do single-photon measurements, or we can do time-of-arrival calculations, or we can count the photons measured in a certain time.

We can use vacuum fluctuations, we measure the quadratures as we saw last time: they have a defined variance, so we can subdivide the pdf of the homodyne measurement into equal-probability regions.

7.3 Semi device independent QRNG

How do we distinguish the randomness of a quantum superposition from the randomness of a mixed state? We can rotate the basis.

If we do this, then we can tell whether the state we are seeing is truly pure. The asymptotic mean entropy is lower in the two bases: the state was not truly pure.

We can also have a measurement-device independent measurement.

We can also do dimension-witness QRNG: we only assume that the state is a qubit.

7.4 Fully device independent QRNG

We certify the entanglement by the violation of Bell's inequalities.

LAB: tomogaphy + QKD with entangled photons. We will estabilsh the dates at the end of April, depending on whether the labs can reopen or not.

8 Quantum Communications Move to Space

Tuesday 2020-5-12, compiled May 12, 2020

Today we want to show how quantum communications can be performed at very long distances, and how this can be used to investigate quantum foundations. We will see some examples.

We need to measure qubits in order to gain physical insight: depending on the kind of measurement we perform we get different results. **Quantum communication** is about sharing a quantum state between distant partners.

We have the usual naming conventions: Alice, Bob and sometimes Charlie want to communicate, while Eve wants to disrupt.

There is a European project called Open QKD. It tries to find applications of quantum communications to various practical scenarios.

The Holy Grail of cryptography is **unconditional security** in communication.

We need to describe the degrees of freedom in our system. We use degrees of freedom which are resistant to propagation: examples are polarization modes and temporal modes. For this, we need an adequate spectral support.

Modes connected to angular momentum decay too quickly for true long-range.

What do we want to do with Space Quantum Communications? To date, SQComm have been demonstrated up to LEO. We want to extend this.

The orbits are classified into LEO, MEO and GEO. The low orbits pass by very quickly.

We can derive theoretically how many common qubits M we need in order to get a shared key of length ℓ with a quberr Q.

Satellites are equipped with retroreflectors. This allows for time-of-flight measurements of the photons: so, we can do geodesy, measure precisely the deformation of the Earth's surface.

We can do quantum communication at LEO! We send "control" pulses every 100 ms, and then single photons at 100 MHz.

References

[Bru+14] Nicolas Brunner et al. "Bell Nonlocality". In: *Reviews of Modern Physics* 86.2 (Apr. 18, 2014), pp. 419–478. ISSN: 0034-6861, 1539-0756. DOI: 10.1103/RevModPhys.86.419. arXiv: 1303.2849. URL: http://arxiv.org/abs/1303.2849 (visited on 2020-03-27).

[Sca+09] Valerio Scarani et al. "The Security of Practical Quantum Key Distribution". In: *Reviews of Modern Physics* 81.3 (Sept. 29, 2009), pp. 1301–1350. ISSN: 0034-6861, 1539-0756. DOI: 10.1103/RevModPhys.81.1301. arXiv: 0802.4155. URL: http://arxiv.org/abs/0802.4155 (visited on 2020-03-20).

[Tis19] J. Tissino. *Quantum Information Notes*. Course held by Simone Montangero at the university of Padua. 2019. URL: https://github.com/jacopok/handbooks/blob/master/undergrad/quantum_info/quantum_info.pdf.