

Quantum optics

Jacopo Tissino

March 20, 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 mechanics.

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:

$$\nabla \times E = -\frac{\partial B}{\partial t} \quad (1)$$

$$\nabla \times B = \mu_0 \epsilon_0 \frac{\partial E}{\partial t} \quad (2)$$

$$\nabla \cdot B = 0 \quad (3)$$

$$\nabla \cdot E = 0, \quad (4)$$

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

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

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

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

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

Then, the Hamiltonian can be shown to be

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

In order to quantize the field, we use the correspondence principle to replace $p \rightarrow \hat{p}$ and $q \rightarrow \hat{q}$. 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 annihilation operators:

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

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

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

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

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

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

$$\frac{d\hat{a}}{dt} = \frac{i}{\hbar} [\hat{H}, \hat{a}] = -i\omega\hat{a}, \quad (12)$$

so the evolution is given by circular motion.

If $|n\rangle$ is an eigenvector of \hat{H} with energy E_n , then $\hat{a}^\dagger |n\rangle$ 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

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

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

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

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

$$\sum_i |i\rangle\langle i| = \mathbb{1}. \quad (15)$$

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*,

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

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

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

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

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

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

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

and we define the quadrature operators:

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

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,

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

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

$$\rho = \frac{1}{\text{tr} \exp(-\hat{H}/k_B T)} \exp(-\hat{H}/k_B T); \quad (22)$$

which gives a familiar result:

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

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

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

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

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

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

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

It can be shown that

$$\langle \hat{n}^2 \rangle = \bar{n} + 2\bar{n}^2 , \quad (27)$$

which implies

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

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

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

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

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

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

$$|\alpha\rangle = C_0 \sum_n \frac{\alpha^n}{\sqrt{n!}} |n\rangle . \quad (30)$$

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

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

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

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

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 $|\alpha|^2 = \bar{n}$.

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

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

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

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

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

We can define the displacement operator:

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

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:

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

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

$$\hat{A} = . \quad (37)$$

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

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

which can never be zero: its square norm is $\exp(-|\beta - \alpha|^2)$ 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

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

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 sandwiching 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

$$\frac{|\langle \text{emission} \rangle|^2}{|\langle \text{absorption} \rangle|^2} = \frac{n+1}{n}, \quad (40)$$

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 the deexcitation is given by

$$w_i = \frac{\bar{n}}{t_{\text{sp}}}, \quad (41)$$

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

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 $0 \rightarrow 3$ 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 $3 \rightarrow 2$. The $2 \rightarrow 1$ 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:

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

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 $N = W t_{\text{sp}}$.

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

$$\Phi = \frac{I}{h\nu}, \quad (43)$$

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

$$\frac{d\Phi}{dz} = \gamma(\nu)\Phi(z), \quad (44)$$

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

$$P_i = \chi_{ij}^{(1)} E_j + \chi_{ijk}^{(2)} E_j E_k + \dots, \quad (45)$$

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

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

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

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

with M being a unitary matrix:

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

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

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

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

$$|0\alpha\rangle \rightarrow \left| i \frac{\alpha}{\sqrt{2}} \right\rangle \otimes \left| \frac{\alpha}{\sqrt{2}} \right\rangle, \quad (50)$$

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*.

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

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

Monday
2020-3-16,
compiled
March 20, 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:

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

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

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

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

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

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

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

$$= \frac{1}{\sqrt{2}} [c_H^\dagger d_V^\dagger - c_V^\dagger d_H^\dagger] |0\rangle, \quad (57)$$

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:

$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}} [a_H^\dagger b_V^\dagger \pm a_V^\dagger b_H^\dagger] |0\rangle \quad (58)$$

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

and with similar steps as before we get that for the ψ^\pm states (singlet) the photons come out in different states, while for the ϕ^\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 ψ^\pm (or ϕ^\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

$$|\varphi\rangle_A = \alpha |0\rangle + \beta |1\rangle, \quad (60)$$

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

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

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

so if we compute

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

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

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

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

The $\frac{1}{2}$ factor accounts for the normalization of the probabilities of obtaining the various states: regardless of $|\phi\rangle$, 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:

$$\frac{1}{4}|\phi\rangle\langle\phi| + \frac{1}{4}\sigma_x|\phi\rangle\langle\phi|\sigma_x + \frac{1}{4}\sigma_y|\phi\rangle\langle\phi|\sigma_y + \frac{1}{4}\sigma_z|\phi\rangle\langle\phi|\sigma_z = \frac{1}{2}\mathbb{1}. \quad (65)$$

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

$$\mathbb{1} \rightarrow \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\psi^-\rangle \quad (66)$$

$$\sigma_x \rightarrow \frac{1}{\sqrt{2}}(|11\rangle - |00\rangle) = |\phi^-\rangle \quad (67)$$

$$\sigma_y \rightarrow \frac{1}{\sqrt{2}}(|11\rangle - i|00\rangle) = |\phi^+\rangle \quad (68)$$

$$\sigma_z \rightarrow \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\psi^+\rangle, \quad (69)$$

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

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle? \quad (70)$$

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

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

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

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 $|\psi_\alpha\rangle$ we can do

$$\mathbb{P}_\alpha = \langle \rho | \psi_\alpha | \rho \rangle = \sum_\mu r_\mu \langle \Gamma^\mu | \psi_\alpha | \Gamma^\mu \rangle = \sum_\mu r_\mu B_{\mu\alpha}, \quad (72)$$

and this system is solvable as long as the projectors $|\psi_\alpha\rangle\langle\psi_\alpha|$ 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

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

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

$$r_z = P_0 - P_1 \quad (74)$$

$$r_x = 2P_+ - 1 \quad (75)$$

$$r_y = 2P_1 - 1, \quad (76)$$

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
March 20, 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 . If they use the same basis, Bob measures the same thing Alice sent.

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

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 $|\Psi^-\rangle$.

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

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

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 $|\Psi^-\rangle$. 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 $|\Psi^+\rangle$; 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

$$r = I_{AB} - I_E, \quad (78)$$

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:

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

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

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

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

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

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

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

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

$$I_E = h_2(Q). \quad (83)$$

With the 6-state coding we have

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

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:

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_n \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (85)$$

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.

References

- [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](https://doi.org/10.1103/RevModPhys.81.1301). arXiv: [0802.4155](https://arxiv.org/abs/0802.4155). URL: <http://arxiv.org/abs/0802.4155> (visited on 03/20/2020).
- [Tis19] J. Tisino. *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.pdf.