

The following content is provided under a Creative Commons license. Your support will help MIT OpenCourseWare continue to offer high-quality educational resources for free. To make a donation or view additional materials from hundreds of MIT courses, visit MIT OpenCourseWare at ocw.mit.edu.

PROFESSOR: Good afternoon. So, we continue our discussion of quantum states of light, and we focus on single photons as qubits today. But before I get into this, I want to ask you if you have any questions about the last unit we be completed on Wednesday-- namely, the discussion on non classical light-- in particular, squeezing light-- and we also discussed a lot of exciting quantum mechanical effects related to beam splitters.

So, any questions? Anything you would like to see discussed? So, as I pointed out, we want to now talk about realization of quantum logic and quantum gates with single photons, but I also said that we are actually using the language of quantum communications-- a kind of information processing to describe general physics in a very nice way.

So, first-- when we talk about photons, we should talk about our qubits, and right now, you may think that having a single photon and having no photon in a mode are two possibilities. And you could use them as qubits. However, I will tell you today that it is better, actually, to use always one photon, but in two different wave guides-- two different modes. But, we'll get there in a moment.

So, the first task at hand is we want to manipulate photons. And for that, I want to introduce phase shifters and beam splitters. And just to give you the punchline right away, what I want to show you is that those two simple devices -- beam splitter, a half-silvered mirror, a phase shifter, which is just a piece of glass which you can put into one of the laser beams-- that those two elements and those two basic operations, if they are now put together-- if you do a beam splitter, a phase shifter, another beam splitter and such-- you can realize any single qubit operation.

Therefore, if you have our qubit cubic state with single photons, any possible state of those qubit can be realized using these optical elements. Therefore, when I say we want to realize how we can manipulate photons with optical elements and such, I'm not going for a zoo of optical elements. Those two will do it all. So, with the phase shifter, that's what we discussed at the end of last class. If you have two modes, and we shift the phase in one of the modes, just simply put a piece of glass into it, then there is a phase shift.

And why do we need two modes? Well, phases are usually-- at least in experiments-- not absolutely defined. You need a phase reference, and here, the mode a acts as a phase reference. Let me address one question which a student asked me after class, and this was related to what phases appear in more than one place. The student's question was motivated that if you have one photon, it's a flux state.

A flux state is a circle in the causal probability, and therefore, the electric field has no phase. Well, this is the phase of the electric field, but here, we're talking about the phase of the wave function. And a flux state within photons is an eigenstate of the harmonic oscillator. It has a time dependence, $e^{-i\omega t}$, and we can change its phase. So, this is a kind of phase shift I've introduced here.

So, the second element we need to realize-- arbitrary single qubit operation is the beam splitter, and I introduced a beam splitter by just saying, hey look, I think that's a good Hamiltonian. Let's see what this Hamiltonian does to the two modes, and then we realize-- yes, it takes those two modes, and it mixes the modes with cosine theta sine theta reading factors. That's exactly what you expect a beam splitter to do.

I'm not sure we need here now because it's part of your homework assignment. You will show that if you have a coherent state, the coherent state is split by a ratio which is cosine square theta sine square theta. So, it's exactly what you'd expect from a beam splitter. So from that, you realize now what this angle theta is, which I just put into the Hamiltonian. The cosine square and sine square of it is the

reflection and the transmission of the beam splitter.

Any questions at that point? Let me now introduce matrix representation, which will come in handy. You remember that you transform an operator-- the mode operator, the annihilation operator a and b . We multiply with the beam splitter operator on the left and on the right, b dega-- b ab dega. But there is often a simpler way how the right inside can be written, and this is by using a matrix representation, which goes as follows.

We can say that the two operators are transformed by the following matrix, and this matrix represents the beam splitter. So that's what the beam splitter does to the mode operators. Now, we want to talk about what does the beam splitter do to quantum states, to single photon states. So now, we want to transform the single photon states.

It's a little bit like, well-- we know what to do in the Heisenberg picture to the operator, but now, we want to see what happens to the wave functions. So, now-- I want to say it very slowly, because it shouldn't lead to any confusion later. We have single photons-- we can have the single photon in mode b , or we can have it in mode a . These are the two possibilities. And right now, I label it like this-- where the first number is your occupation number of mode a , and the second number is your occupation in mode b .

You have to be a little bit careful-- I'm just saying that keep your alert level high. Later, I will use qubit representation, where the qubit one means the photon is in mode a , and the qubit zero means the photon is in mode b . So when we talked about logical states of our two levels used, and the photon can be here or the photon can be there, zero means the photon is there. It doesn't mean that we have zero photons. But sometimes, I have to talk about the photons-- and that's what I'm doing right now-- and zero means no photon in this mode. But I will remind you of that as we go along.

So we have the two quantum states-- one zero, and zero one. And let's just see what the beam splitter is doing to one photon in mode b . I'm changing notation from

one line to the next in my notes. Just give me a split second. Yes. So, let's use this convention. So, just to elaborate what I just said is-- this convention one zero is the direct product of the Hilbert space for mode b , with one photon with the Hilbert space of mode a , and we have zero photons there. And sometimes, you want to denote the state by putting a comma in between. That's all the same.

So, how do we transform the quantum state with the beam splitter operator? Well, we could now apply to the quantum state, but we just learned how to apply to operators, so let's just use what we already know, because we can write the state like this. And now, we want to insert the unit. We want to insert the unit operator b b^\dagger , and now, we can use our knowledge of the operator. We know how this transforms. We had this above the transformation of the operators b and b^\dagger , and when we apply b to nothing-- to no photons, we get no photons.

So now, by taking from the page above the transformation of the operator b^\dagger , it's a linear combination of a^\dagger and b^\dagger . We find what we expect-- the photon can now be in the same mode, or it can appear in the other mode. And the coefficients from the transformation of $\cos\theta$ minus $\sin\theta$. And if you would send the other state through the beam splitter, we find the $\cos\theta$ $\sin\theta$ component.

So, since the total probability to have a photon is $\cos^2\theta$ plus $\sin^2\theta$ is unity, we find what we expected, but it's nice to see it. Namely, that b conserves the photon number-- of course, this should have been obvious from the outset, because we used a Hermitian operator, a unitary time evolution, and that is energy-conserving.

What happens if we use a state which has one photon in each mode, and we act on it with the beam splitter? Well, it gives a superposition of the two photons can now be in either of the two modes, or they can be distributed one in each mode. And the coefficients are because we have two transformations, products of \sin and \cos . Here is $\cos^2\theta$ plus $\sin^2\theta$. Here is a plus $\sin\theta$, square root two plus square root two.

So that means if we allow one photon to be in each mode, it leads us actually out of the Hilbert space of single photon states, because we have a certain probability now that we have two photons in each mode. So, we don't want that. So if you want to deal with only one photon, we should restrict our attention, our formalism to the states which have no more than one photon. And now, if we act on those states with beam splitters, we don't get out of this subspace or fill that space.

However, we also want to omit this state because it's more elegant to do it, but also, if you have a single photon state and we have a detector which has not 100% efficiency and we do a measurement-- well, we don't know if we have the state zero one, but we just didn't detect it, or we had the state zero zero. Whereas if you deal with two states where you always have a photon-- exactly one photon-- and you read out your system and you detect nothing, well you discard the measurement. And then, you only take the measurements which have detected one photon. So you have the ability to deal with finite efficiencies and losses in a very straightforward way.

Yes?

AUDIENCE: The operation of dega 1, 1 doesn't look so unitary to me.

PROFESSOR: Yes. And it is in my lecture notes. Minus.

AUDIENCE: [INAUDIBLE].

PROFESSOR: Yes. And it's right in my lecture notes. Sorry. Sometimes, when you're talking, explain it, build it up-- yes. Thank you. Other question? Good.

So what I just said, that we want to restrict the Hilbert space to exactly one photon, this is so important for implementations and discussions of quantum information protocols that it has its own name. It's called the dual-rail photon state. The dual-rail photon state space. Exactly one photon, but the photon can either be in mode a or in mode b. So this part-- this dual-rail photon state space-- is a Hilbert space which has a basis which is zero one and one zero, and this is of course a two-level system.

In this so-defined Hilbert space, we can have an arbitrary state, $|\psi\rangle$ which is-- as in any two-dimensional Hilbert space-- it's a linear superposition of your two base states with coefficients alpha and beta. And the few of them for which we have prepared right now is that any possible state of this Hilbert space can be created from any of the base state, that is from zero one simply by beam splitters and phase shifters.

When I taught this unit the last time, I went through the proof, but I want to make room for more in-class discussion like we had on Wednesday with the clicker question, so what I decided is I give you the idea behind the proof, and the formal parts you can simply fill in by reading about it on the Wiki page.

So, let me just focus on the idea. So the proof is that if I use some column vector for alpha beta-- that we can identify with the beam splitter and the phase shifter-- we can identify them as rotation operators. This is immediate obvious if I use the transformation on psi by beam splitter, we learned just a few minutes ago how the beam splitter operator acts on the base state. So now, we know how it acts on an arbitrary linear combination. And the matrix here is nothing else than the rotation matrix with the minus sign around the y-axis. So that's a beam splitter.

The phase shifter is not changing any state. It shifts one of the states by $e^{-i\phi}$ to the minus $i\phi$, but I can sort of summarize it by taking half of it out as a prefactor, and then adding here $e^{i\phi/2}$ to the $i\phi$ over two. And this here is immediately recognized as the rotation matrix around the z-axis.

Now, you may ask what about this? Well, this is an irrelevant global phase factor. If you have any state in Hilbert space and you change the global phase, it doesn't matter. Therefore, we are realizing that the beam splitter is a rotation around the y-axis. It's now a definitional thing, but we put a factor of two here by an angle two theta, and the phase shifter is a rotation around the z-axis by an angle phi.

Now, with that, we can formulate what is called Bloch's theorem, that any unitary operation of a two-dimensional Hilbert space can be written as a product of

rotations. Now, let's first count an arbitrary unitary operation while a two by two matrix in complex space has eight numbers-- four real parts, four imaginary parts. But if the matrix is unitary, they are only four independent elements-- alpha, beta, gamma, delta. And if you parametrize the unitary matrix with alpha, beta, gamma, delta which is shown in the weekly notes, then we can write this arbitrary unitary matrix by a combination of an overall phase factor. Which is irrelevant because it's a global phase factor-- and then a rotation around z, a rotation around y, and a rotation around the z-axis.

So, if I rephrase this theorem in modern language, I would say we have a qubit which is a two-level system characterized by two numbers alpha beta. And we can do an arbitrary operation in the Hilbert space of the qubit, which is called an arbitrary single qubit operation. So, can be performed by phase shifters and beam splitters.

Just to make sure that this doesn't lead to any confusion, the phase shift which is relevant for this Hilbert space is a phase shift which is relative between the two states, and can be detected by an interference experiment. Those global phase shifts cannot be detected. There is no observable, no procedure to observe those-- unless you would have a a third mode. But then, we would expand the Hilbert space to three levels and then, of course, it's the global phase shift in the two-dimension Hilbert space becomes a relative phase shift within the three-dimension Hilbert space.

And in modern language, those single qubit operations are called quantum gates. So, all gates which act on a single qubit can be realized with phase shifters and beam splitters.

Let me give you one example for that. In quantum computation, quantum information science, there is a very important gate-- the Hadamard gate, which is described by a transformation which has $\frac{1}{\sqrt{2}}$. And I said it can be realized with a beam splitter and phase shifter. So let me just show it to you in using our symbolic language. So if you look at the matrix we had derived for the beam splitter,

you realize that we get the Hadamard gate by adding the phase shifter by π .

So, in that sense, single qubit operations are checked off. We know how to deal with that. We want to now move towards two qubit operations-- and then, it's getting really interesting.

As you may know, you can do any arbitrary operation in many qubits by just having single and two qubit operations. Therefore, once we know how two qubits interact-- how photons in two different qubits interact, we are done-- we have universal quantum gates.

The element I need for two qubit operation is the Mach-Zehnder interferometer. Just a side remark, I introduce a Mach-Zehnder interferometer here as a way to manipulate qubits. On the other hand, most of you know that interferometers for light and interferometers for atoms are used for some of the most precise measurements ever done.

So, in that sense, this shows the dual use of the formalism I'm introducing here. We really use some of the formalism and the language we develop here for qubit operation, and discuss next week the ultimate accuracy-- the fundamental limits to the accuracy you can get in precision measurements based on interferometry.

Let me just write down the sentence because it has a lot of key words in it. So the dual-rail photon presentation of a qubit-- this is what we have achieved so far. So this allows us now to discuss interferometers simply as [INAUDIBLE] gates. And what isn't interferometer-- an interferometer is, in its basic [INAUDIBLE], you have a beam splitter, you have two paths, and then you use another beam splitter which recombines the two beams.

So, let me draw two beam splitters. These are two beam splitters. We have an input [INAUDIBLE] b , an input mode a . They are sort of mixed. Here are the two arms of the interferometer. And now, we create output modes b prime and a prime. What we have introduced here is the beam splitter b , and by putting the dot on the other side, this is b degra. Since b degra times b equals one equals the identity, this

interferometer is doing nothing. If the photon starts in mode b, it comes out in the upper mode b. If it starts in a, it comes out in the mode a.

But of course, this is just the beginning, because we can now introduce here an arbitrary phase shift ϕ . And now, it is an interferometer. Now, we can read out with the output the phase shift, and ultimately, with very high precision. I want you to appreciate that. If we had used single qubits in one mode-- no photon, one photon.

I gave you many reasons why we shouldn't do that, but then, we would be dealing with one mode, and this would actually be something which involves two qubits. But since our single qubit system is a two-level system where the photon is here and there, we can now send single photons with the interferometer-- describe the interferometer as a single qubit operation. At least it's nice. It allows us to keep things simple, and discuss things at a very fundamental level.

So, what we want to figure out-- what is this interferometer doing? So, we want to know if we have an input state-- what is the output state? And the input state can now be any arbitrary wave function in our dual-rail Hilbert space. So, it's always one photon, but it can be in a random superposition in an arbitrary superposition of states a and b.

Well, with the formalism we have developed now, it becomes very simple. All we have to do is we have to act with the first beam splitter with a phase shifter, and with a second beam splitter onto the state. And this is nothing else than taking two rotation matrices and multiplying them. The beam splitter we have chosen, I said there was sort of a phase convention when I peeked the beam splitter. It is a rotation by $\pi/2$. This is minus $\pi/2$, and the z-rotation is by minus ϕ .

I'm not sure if I manage to do that, but if this is the y-axis and we start with the qubit, the first beam splitter rotates it down. Then, the rotation by z-- thus, that-- and the second beam splitter rotates by ϕ . Therefore, the qubit is like that. Therefore, if you count all x's with the things I did is-- I started with a qubit here. It went down like this, like this. So what I did is-- in the end, I simply rotated it around the x-axis.

If you want, you can multiply the matrices, or you can draw block sphere visualization. That you say we have an x-axis, y-axis, and z-axis. So the z is vertical. So, we started out with the qubit along the z-axis. The first one was rotation around the y-axis. So then, we were here. The second operation was rotation around the z-axis. And then, we have to rotate back around the y-axis, which eventually gives this as the final state.

So ultimately, the product of all this is a rotation around the x-axis. Our interferometer-- I'm not sure if you've ever heard the language, but it's really elegant and powerful. An interferometer with an arbitrary phase in this two-level Hilbert space with this sort of geometric interpretation we have given, is nothing else than a rotation around the x-axis.

Therefore, we know immediately the two limiting cases when we rotate by zero, it's sort of balanced. Output and input are the same, because we're not rotating at all. Whereas if we have a phase shift of 180 degrees, we swap the two qubits. So, we swap the two modes, and swapping modes is an inversion of the qubit.

So that's almost trivial, but we need this definition-- we need this knowledge to take it to the next step. Remember, we want to do something more interesting than rotating two level systems. We want to get two qubits, combine them, entangle them, and all that. So what we need for that is-- we have to expand the Hilbert space.

I introduced the Mach-Zehnder interferometer as the device to do it. But now, we need a way how a second photon from another qubit can interact with the photon of our first qubit. And we want to do that by introducing first the non-linear Mach-Zehnder interferometer. I want to throw in a non-linear element, and then we are ready to allow the second qubit through the non-linear element to manipulate the first qubit. And then, we have interactions between qubit. We have two qubit gates.

Let me maybe just deviate for my notes. I really want to show you what I'm doing, and that you have it clearly in mind where I'm aiming it. So what we want to accomplish is-- instead of having a phase shifter with an externally controlled phase,

I want to put in some non-linear crystal-- which has an index of refraction which has a phase shift. But now, the fact that the non-linear crystal has the property, that its index of refraction changes when I take another laser beam and send it through.

So, the laser beam through-- because the index of refraction is intensity-dependent, the green laser beam changes index of refraction of the non-linear crystal-- also called Kerr medium. And that means now, because the blue beam goes through the same crystal, that the green beam controls now the phase shift of the blue beam. And now, we have interacting photons-- one photon interacts with the second photon.

Let's work it out. So our goal is to develop a description for non-linear Mach-Zehnder interferometer. What we need is a non-linear medium. So, let me just introduce for two or three minutes non-linear medium, how we describe it, and then we put it into our interferometer. So, in linear optics-- just to remind you, we have a polarization on electric dipole moment, which is proportional to the electric field of light, and χ_i is the polarizability.

The most complicated case, it can be polarizability tensor. Now, this is linear. If you want two non-linear, then we have the linear relationship simply as you can say the first terminal [INAUDIBLE] expansion. So we expand the response of the medium in powers of the electric field, and we have the susceptibilities χ_1 , χ_2 , χ_3 , and so on.

We have already encountered a non-linear element which had a χ_2 susceptibility, and these were the crystals we put in our OPOs into our optical parametric oscillators. Remember, the optical parametric oscillator involved-- how many modes? Three. We had one photon, which was broken down into two photons. But that also means that the reverse process is you drive the beam-- you drive the OPO with ω , but the e^2 term creates an electric polarization as 2ω . And if you have an oscillating polarization as 2ω , you create light at 2ω .

So, I just want to remind you that the χ^2 term is what we have already encountered. That's not what we need for the non-linear Mach-Zehnder

interferometer. What we need now is a χ^3 interaction, which is the Kerr medium. Because we want to realize the following Hamiltonian.

The Hamiltonian, the Kerr medium is also called cross-- that's $\chi^{(3)}$ -- cross-phase modulation. One beam can affect the phase of another beam, and this is called cross-phase modulation. There's also self-phase modulation-- that one laser beam changes the index of refraction for itself-- but here, we want the cross-phase modulation.

So, we know that if we have a mode, and we shift its phase, we're not changing any photons. So if we're in an eigenstate of mode a with one, two, or three photons and we simply shift its phase, we are diagonal in a $\text{dega } a$, and the phase shift is proportional to prefector here . So this Hamiltonian is simply a phase shift for photons in mode a , but if you now multiply that with $b \text{ dega } b$, the phase shift is now proportional to the number of photons in mode b .

Now, we have a situation that the phase shift from mode a proportional to the intensity in beam b , and vice versa. So, I think it's self-evident that this Hamiltonian is sequential description of the process we want to introduce know.

This is the cross-phase modulation Hamiltonian. Isn't it much more elegant to describe non-linear optics with Hamiltonians than with parametrized susceptibilities and all that? It's just amazing-- you write in a few letters and it has all the power of the classical description-- plus extra, because it includes quantum fluctuations and everything. I hope you appreciate the power of the language we are developing. This is the cross-phase modulation Hamiltonian.

And now, we want to use this Hamiltonian in a crystal of lengths L . Well, you know if you have a time-propagation operator, you put the Hamiltonian in the exponent and multiply with t , but for propagating laser beam, t and L are related, so this is now the unitary transformation if you propagate through that crystal.

We are now defining that by saying we have this non-linear susceptibility, things will be proportional to the links L , and then we have the operator $a \text{ dega } a, b \text{ dega } b$.

And let me choose for the following discussion that the links are chosen, such that-- when multiplied with a non-linear susceptibility, we get a phase shift of π .

Now, we are ready to describe what happens when we have a Kerr medium, and we have two input modes. So, let's write down the table of possible combinations and operations.

Well, when we act on the vacuum, we get nothing. What happens when we have one photon in one mode? What happens to that photon? Well, the extra phase shift coming from cross-phase modulation is zero, because we have no photon in one of the modes, and a $\text{dega } a$ or $\text{dega } b$ acting on this mode gives zero.

Therefore, as long as we have only one photon, we have no phase shift. The exponential factor is one, and we simply reproduce the original state. So, the only non-trivial situation by construction is when we have one photon in each mode, and then we get the matrix element e to the ikl . And we adjusted the lengths of the crystal that this is just minus one.

In other words, in this Hilbert space, we get a phase shift of π -- we get a minus sign when we have one photon in each mode. That's all what this medium does. And if you ever thought about it-- how to deal with this situation-- that when I said there is one photon which provides a phase shift to the other photon. But the other photon is also providing a phase shift to the first photon.

So you may wonder. When you have a combined state of the two, how do you deal that one photon shifts the other photon, and vice versa? But when you apply the operator, you don't even have to think about it. You see that the operator for the combined Hilbert space of the two photons gives you a phase shift of π . It's not π for one photon times π for the other one-- it's π for the whole quantum state.

Any questions? We have a Kerr medium, which means we are ready now to put it into our interferometer. I'm doing at this time-- insert picture.

This is what you want to do now. We have now three modes of light. You would say, hey-- a qubit, each qubit is two. What is it-- is it one and a half qubit? Yes, it is-- but

we extended two cubits in a moment. So what we simply have right now is we have the mode c -- which controls the non-linear medium, and we have what we have already discussed. Our interferometer with a phase shifter, which is now the Kerr medium.

So I think even without doing any math, we know that by construction, when we have no photons in c , that the modes a prime b prime transform-- become a and b , because we have a balanced interferometer which is the identity transformation, unless we have a phase shift.

But when we have one photon in state c , then we actually swap. So, that's pretty cool. A single photon in mode c will redirect the photon from ab to ba . So that's how one photon in mode c controls what happens to the photon in ab . If you want a general description of that, we obtain the output state from the input state by using the matrix b .

This was our interferometer based on two beam splitters. It involved mode a and b . But now, we throw in the phase shifter, which is our Kerr operator-- our non-linear phase shifter with b and c . This new addition to the interferometer is described by e to the i , non-linear susceptibility L , b dega b , c dega c .

Let me give you one intermediate result. We have now beam splitters on either side. And that leads us to an expression. While the beam splitters do nothing to the mode c , but the beam splitters transform the modes in linear combinations.

And if you do some tedious rearrangement of terms-- more details are given in the Wiki-- you find that the essential result is now the operator, which we get is $\frac{1}{2}(\text{dega } b \text{ minus } b \text{ dega } a)$ over 2.

I'm not giving you the non-essential terms, which are just phase shifts-- global phase shifts. So, let me write it down in blue here. This is just the result of the operator manipulation. If I would cover that-- what is that? Do you remember $\frac{1}{2}(\text{dega } b \text{ minus } b \text{ dega } a)$ in the exponent? It's a beam splitter. And the beam splitter-- the beam splitter matrix was $\begin{pmatrix} \sin \theta & \cos \theta \\ \cos \theta & -\sin \theta \end{pmatrix}$. So we had a θ here.

Now, you realize that this non-linear Mach-Zehnder interferometer, the three optical elements can be replaced by simply a single-beam splitter for mode a and b, but the angle θ of the beam splitter is now controlled by the photon field in state c.

In other words, we have now a beam splitter. I told you that a beam splitter is nothing else than a rotation around the y-axis. So now, this non-linear Mach-Zehnder interferometer is simply a beam splitter with a rotation angle given by this term.

Any questions? This is a situation we just had, and we can now get to two qubits by simply adding one more rail. Remember, two rails with exactly one photon in it is a qubit.

So now, we have a qubit here, and we have a qubit there. And you see immediately one way how the upper qubit x on the lower qubit-- if the lower qubit has a photon in state c, it flips the other qubit. But if the upper qubit has a photon in d, it doesn't do anything to the lower qubit.

Now, we have a two-qubit operation. This is shown here. But what I want to discuss now is the situation when we throw in one more beam splitter, and this beam splitter acts on the upper qubit.

Well-- isn't it great how quickly we go from simple elements to something which looks quite sophisticated? So, this device now is a single optical device which can entangle qubits, which leads to entanglement.

And actually, entanglement is our next big topic we want to talk about-- entanglement between particles, entanglement between photons. And by introducing the Mach-Zehnder interferometer, I was actually building up the situation, which is extremely simple elements which lead to entanglement. We have everything for the description-- each of those elements is described by a matrix which we have developed.

Therefore, by just multiplying those matrices, you find immediately how this whole

device is now manipulated into qubits. So, if you want, you can just take the crank, use what we have already done, and crank out the result for it.

Now I wish I had a bigger screen, because I want to describe what's going on for you. What I want to discuss with you now is what happens when we take this device, and we use exactly the states $|0,1\rangle, |0,1\rangle$ at the input as I indicated.

In terms of qubit language, I say that the first qubit is in spin-up, and the lower qubit is also in spin-up. Spin-down would mean that the single photon is in the other state. Our two-level system-- our dual-rail single qubit two-level system is the photon can be either in one of those states. This one, we call spin-up-- this one, we call spin-down.

What I want to discuss with you now, what happens when we start with this symmetric input up-up, which means $|0,1\rangle, |0,1\rangle$. And since I don't want to scroll up and down so often, everything is trivial beam splitters, except for the situation when we have one photon each here, and then the Kerr medium gives us a minus sign. So that's what I want to put in.

Remember, I want to develop the physics in one, two, three temporal steps. The first temporal step is simply two beam splitters, and this is shown here. We start out-- and now we have beam splitter for the upper qubit, beam splitter for the lower qubit. And well, by just multiplying it out, we are now obtaining this summation state for the four different modes.

And I'm dropping here factors of square root-- or you can collect them at the end, if you want. And I said the only interesting situation is where we have two photons-- one each in the two middle modes, because now, the Kerr medium kicks in and gives us a minus sign. Now, you can show by inspection that if you now apply the beam splitter to modes a and b, you take $|1, 0\rangle$ into a linear combination of $|1, 1\rangle$ and $|1, 1\rangle$, but the beam splitter is only acting on the last two numbers here. Then you obtain a state which looks very simple. So this is the output state of the device.

Any questions? And this output state is-- if I use the spin language, it's an entangled

state. So now, you have one simple example how just using linear optics, very simple elements you can start with one photon here, one photon here, a simple product state, and what comes out is an entangled state.

Questions? Let me tell you what I'm not telling you-- namely, the Wiki developed by a professor [INAUDIBLE] has now a wonderful section on a famous quantum algorithm-- the Deutsch-Jozsa algorithm. Pretty much using the elements we discuss, you can now realize the Deutsch-Jozsa algorithm, which is one of the famous algorithms where quantum logic-- quantum computation is faster and more efficient than classical computation.

I decided not to present it to you, because it just leads to an even more complicated diagram and more formulae. You should just sit back and slowly read it by yourself. There is no new idea introduced-- it's just the concepts we have discussed can lead to very powerful algorithms. What I want to rather do is-- I want to continue our discussion and now talk about the object we have encountered here-- namely, entangled states. But if you have any questions, if you want me to explain anything more about the single qubit manipulation, the dual-rail photon state, I would be happy to do that.

Our next chapter is on entangled photons, and what we can accomplish in the next 10 or 15 minutes is mainly a definition and some of the properties. What we will do next week is we will talk about how we measure entanglement-- you already had one homework assignment where you discussed one way to measure entanglement, but there are others which we want to discuss next week.

I also want to show you next week how entanglement leads to the Einstein-Podolsky-Rosen paradox and Bell's inequalities. And eventually, I want to show you how you can entangle not only photons, but how you can entangle atoms. But that's an outlook. I think, first of all, we want to understand what is entanglement. Entanglement is-- let me first [? motivate ?] it.

Many people regard entanglement as the most quantum essence you can find. Well, there's always a discussion, but it's really quantum. Some people would say

waves are quantum. But often, we find quantum systems-- very famously, Bose-Einstein condensates, which really behave like electromagnetic waves. They can be split. They can interfere. But Bose-Einstein condensates are so big, have so many atoms that you hardly ever encounter quantum fluctuations.

You're really in the classical limit of matter waves, and I would actually say this is maybe not at the heart of quantum mechanics. While it's nice, it's powerful, it's important-- but this is not really the new feature which quantum mechanics has shown us in nature. You would say-- well, what else is quantum? Maybe certain quantum fluctuations going down to single photons, and I would agree that's a quantization of the electromagnetic field. That's much more quantum than having millions of condensates, millions of condensed atoms in one single wave.

But what I would say is even more quantum than the single photon is the entanglement. Entanglement is sort of pure quantum mechanics. With single photons, you can still use intuition. But with entanglement, that is really bizarre. This is really- I hate the word, but let me use it-- this is sort of pure quantum weirdness. And there are people who have spent most of their career until now to just show the weirdness of quantum mechanics, and showing to what peculiar phenomena entanglement leads.

So entanglement has really lead to a lot of-- I should be careful with the word surprising-- surprising always means you didn't have enough imagination to think about it, but yes, I would say-- really truly unanticipated, and in that sense, surprising developments. Entanglement is, therefore, for me, the most quantum aspect of quantum mechanics.

It was through the Einstein-Podolsky-Rosen argument-- it was actually Einstein-Podolsky-Rosen in the '30s who argued-- Einstein-Podolsky-Rosen were really the first-- this was almost 5 or 10 years after the development of quantum mechanics. But it was Einstein-Podolsky-Rosen who looked at the properties of entangled states.

This famous experiment where you have something entangled in position and

momentum space. And then, Einstein-Podolsky-Rosen found a paradox, and their conclusion was that the properties of entangled states implies that quantum mechanics is not complete-- is not a complete description of the world. Well, we don't any longer share this opinion.

It was John Bell and others who said that entanglement really exemplifies that quantum mechanical correlations go beyond classical mechanics-- go beyond the classic picture. Therefore, you can say if you have a quantum system like a Bose-Einstein condensate, where you have end particles doing in unison what one particle does.

This is sort of like the laser where many photons do what one photon does-- but it fits very, very well into the concept of classical probabilities and an intuitive understanding of why many particles do what one particle does. But if the particles are entangled, that's almost like you turbo-charge your system. Your system has now more oomph, more power in it.

And this is shown that it has extra correlation-- there is something extra in it, which you would never get from any classical limit. And this extra oomph, this extra power turns out to be a real resource. So, entanglement-- this extra correlation-- is a resource. And resource means it's good for something. It enables teleportation.

Remember when we talked about the teleportation scheme-- Alice and Bob could only teleport a quantum state because they shared entangled photons. It was this entangled state which Alice manipulated with a measurement, and Bob used this half of the entangled state to recreate the original state. So, it's the engine [INAUDIBLE] up behind teleportation in the world of quantum computation. The exponential speedup of quantum computers versus classical computers in quantum algorithms is due to the entanglement, which we can put into a quantum system.

And eventually, next week, you will see that if you have an atom interferometer with entangled states, we can operate it at a precision which is better than shot noise. So in other words, you use laser light to measure something, and you're limited by the fundamental noise limit of classical physics.

Now, you entangle your laser beam and you get higher precision out of it. So this shows that entanglement is a very special resource. It's very precious, very powerful and can extend what physics can do.

So, let's define it. I'm not describing to you entanglement in the most generous situation. If you talk about many modes-- if you talk about not just pure states, but statistical operators-- it can become quite involved.

I'd rather start with the simple situation, which for conceptual discussions is also the most important one. I restrict our focus now on two modes. I want to ask if you have two modes a -- actually, two modes means two subsystems here. If you have two subsystems a and b -- let me tell you what entanglement is not, and then I make it the definition.

There wouldn't be anything special if you have a system which has two parts a and b . The global system is ψ_{ab} . But if your system would simply factorize into a wave function of subsystem a , direct product with subsystem b , and this here is the tensor product. Then, there would be nothing special going on between subsystem a and subsystem b -- and this is non-entangled. Everything else is entangled. So, this is our definition.

When we have two separate systems a and b , we call this situation the total system bipartite. So, a bipartite state which has sort of half of it in system a , half of it in system b . We need those two different systems-- it's a composite system a plus b . And this state is entangled-- if and only if you cannot find two states ψ_a and ψ_b , such that the state can be factorized.

We need a few examples to fully comprehend this discussion-- what systems a and b qualify. What does it mean if there does not exist any combination? So, let me give you some examples now, and then I think we stop. If you have the $0, 0$ state, photons in two mode, we can factorize it-- and this is not entangled.

If you have a state which is $0, 0$ plus $1, 1$ -- well, you cannot write it as a product of one state times another state. This is entangled. Well, if you take the following state-

- Is that entangled or not? I've written it as a sum of four states, but if you just stare at it for a split second, you realize you can just write it as a product of two states. It's just a product of $0, 1$ with $0, 1$.

So, a state is not entangled if you can write it as a linear superposition of those states. The definition of entanglement is-- if you try hard and hard and hard, and there doesn't exist any product state decomposition, then it is entangled. So, that was easy.

If you use a state like-- let me just leave the $1, 1$ out. What about this one? Well, you can try as hard as you want-- you will not find the decomposition. So eventually, when I say you have to try hard to find decomposition, maybe what we want is we want to apply some operator or some procedure to this state, and get the answer, yes-no. This naturally asks for question-- how in general can we measure if a state is entangled or not? But this is something we'll discuss next week.

So let me just conclude with the following. I'm focusing here and for pretty much all of this course when we talk about entanglement, about pure states. If you have decoherence-- if you have the transition from pure states to density matrices-- it gets much more involved to talk about entanglement and measure entanglement. But at least the basic definition can still be maintained for statistical operators.

If you describe the system-- the total system by one statistical operator-- the system is not entangled. If the statistical operator can be broken up into a direct tensor product of statistical operator for system a and system b. Otherwise, the system is entangled. So the basic definition can be generalized to density matrices, but a lot of things become much, much more messy if you don't have pure states.

Any last-minute questions? See you on Monday.