Quantum information theory (20110401)

Lecturer: Jens Eisert

Chapter 3: Two possible machines

Contents

Chapter 3

Two possible machines

Now that we have had a look at impossible machines to make the point that quantum information is different from classical one and being prepared with the basics, we can turn to discussing possible machines, so machines that are possible within quantum mechanics but which have no classical analog. These schemes are not really applications of quantum information theory as such, but rather paradigmatic protocols, or primitives of more complicated protocols.

3.1 Quantum teleportation

This is one of the most intriguing and paradigmatic schemes. It has a science fiction connotation, and this is not an accident: The idea of teleportation is to "measure" an object, to transmit information and to reconstruct this object elsewhere based on this information. Movies such as the Star Trek series or the Fly have elaborated on this theme extensively. On a more serious note, we know that classical teleportation is impossible: We cannot hope to measure a quantum system, transmit classical information and to prepare a new quantum system on the basis of this information elsewhere: Or if we did, the latter object would necessarily be statistically distinguishable from the former in its quantum state.

3.1.1 Quantum teleportation of qubits

Interestingly, the addition of a single extra ingredients allows to "teleport" in this sense. And possibly unsurprisingly, this additional ingredient is that of entanglement. It is a most paradigmatic scheme that shows how entanglement helps to overcome locality. If this sounds still a bit cryptic at the moment, it will become much clearer later.

For simplicity, let us assume that the input state held by Alice is a pure state of a single qubit. For clarity, let us call this qubit A_1. We will turn to more general prescriptions later. Hence, the input is captured by a state vector

$$\alpha|0\rangle_{A_1} + \beta|1\rangle_{A_1}. \tag{3.1}$$

The index indicates what system we are referring to here. Alice does have this system at her disposal, but she does *not* have to have classical information about $\alpha, \beta \in \mathbb{C}$: To her, this is an unknown state. In addition to this input, both Alice and Bob share a bi-partite quantum system in a maximally entangled state vector

$$|\Phi^+\rangle_{A_2,B} = (|0,0\rangle_{A_2,B} + |1,1\rangle_{A_2,B})/\sqrt{2}. \tag{3.2}$$

B is held by Bob, while A_2 is a second qubit at Alice. This is used as a resource, and as such, often referred to as *ebit* or *entanglement bit*. This is precisely the situation anticipated at the end of the last section. Now Alice performs a measurement on both the input and her half of the entangled pair, so on A_1 and A_2. She does so making use of a maximally entangled basis, so that the projections of the projection postulate reflect the following state vectors

$$\mathcal{B} = \left\{|\Phi^+\rangle_{A_1,A_2}, |\Psi^-\rangle_{A_1,A_2}, |\Phi^+\rangle_{A_1,A_2}, |\Phi^-\rangle_{A_1,A_2}\right\}, \tag{3.3}$$

where

$$\begin{aligned} |\Phi^-\rangle_{A_1,A_2} &= (|0,0\rangle_{A_1,A_2} - |1,1\rangle_{A_1,A_2})/\sqrt{2}, & (3.4)\\ |\Psi^+\rangle_{A_1,A_2} &= (|0,1\rangle_{A_1,A_2} + |1,0\rangle_{A_1,A_2})/\sqrt{2}, & (3.5)\\ |\Psi^-\rangle_{A_1,A_2} &= (|0,1\rangle_{A_1,A_2} - |1,0\rangle_{A_1,A_2})/\sqrt{2}. & (3.6) \end{aligned}$$

This measurement will yield two bits of information, reflecting the four possible outcomes. These outcomes are communicated to Bob. In case she obtains (the measurement outcome corresponding to) $|\Phi^+\rangle$, the resulting state vector is

$$\begin{aligned} & (\langle\Phi^+|_{A_1,A_2} \otimes \mathbb{1}_B)(\alpha|0\rangle_{A_1} + \beta|1\rangle_{A_1}) \otimes (|0,0\rangle_{A_2,B} + |1,1\rangle_{A_2,B})/\sqrt{2} \\ = & ((\langle 0,0|_{A_1,A_2} + \langle 1,1|_{A_1,A_2}) \otimes \mathbb{1}_B)(\alpha|0\rangle_{A_1} + \beta|1\rangle_{A_1}) \otimes (|0,0\rangle_{A_2,B} + |1,1\rangle_{A_2,B})/2 \\ = & (\alpha|0\rangle_B + \beta|1\rangle_B)/2. \end{aligned} \tag{3.7}$$

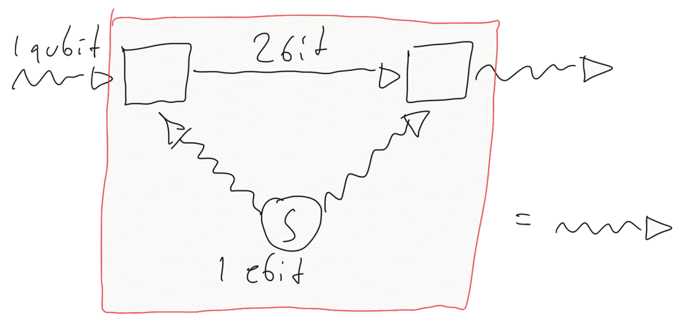
This is only a single line, as the step from the first to the second step is simply the definition of the maximally entangled state vector. The second step is the interesting line. But what a line. Let us recap what has happened here. To start with,

$$(\langle 0,0|_{A_1,A_2} + \langle 1,1|_{A_1,A_2})(\alpha|0\rangle_{A_1} + \beta|1\rangle_{A_1}) = \alpha\langle 0|_{A_2} + \beta\langle 1|_{A_2}. \tag{3.8}$$

And then,

$$\alpha\langle 0|_{A_2} + \beta\langle 1|_{A_2}(|0,0\rangle_{A_2,B} + |1,1\rangle_{A_2,B}) = \alpha|0\rangle_B + \beta|1\rangle_B. \tag{3.9}$$

But the key point is: The latter state vector is one held by Bob! It may help to add the indices. So after the measurement, and Bob knowing that this specific outcome has occurred, the state is the same as the input: The output is hence statistically indistinguishable. Note that also Bob will have no classical knowledge about the unknown state, just as Alice had no information. But Bob can now perform a measurement and use the particle exactly as if the same system had re-appeared at Bob's side. The state has been "teleported".



It is also easy to see what happens if Alice obtains a different outcome. For example,

$$\begin{aligned} & ((\langle\Phi^-|_{A_1,A_2} \otimes \mathbb{1}_B) \otimes \mathbb{1}_B)(\alpha|0\rangle_{A_1} + \beta|1\rangle_{A_1}) \otimes |0,0\rangle_{A_1,A_2} + |1,1\rangle_{A_1,A_2})/\sqrt{2} \\ = \ & (\alpha|0\rangle_B - \beta|1\rangle_B)/2. \end{aligned} \tag{3.10}$$

This is not the same as $\alpha|0\rangle_B + \beta|1\rangle_B$. But given that Bob has received the measurement outcomes, he will know that this specific outcome has occurred, and will be able to make a correction. It is easy to see that

$$Z(\alpha|0\rangle_B - \beta|1\rangle_B) = (\alpha|0\rangle_B + \beta|1\rangle_B), \tag{3.11}$$

where Z is a Pauli operator. Since this is unitary, it can be implemented by Bob as a unitary operation: In fact, this is the first encounter of a quantum gate. In this way, one finds

$$\begin{aligned} ((\langle\Phi^-|_{A_1,A_2} \otimes \mathbb{1}_B)(\alpha|0\rangle_{A_1} + \beta|1\rangle_{A_1}) & \otimes |0,0\rangle_{A_2,B} + |1,1\rangle_{A_2,B})/\sqrt{2} \\ & = Z(\alpha|0\rangle_B + \beta|1\rangle_B)/2, \quad (3.12) \\ ((\langle\Psi^+| \otimes \mathbb{1}_B) \otimes \mathbb{1}_B)(\alpha|0\rangle_{A_1} + \beta|1\rangle_{A_1}) & \otimes |0,0\rangle_{A_2,B} + |1,1\rangle_{A_2,B})/\sqrt{2} \\ & = X(\alpha|0\rangle_B + \beta|1\rangle_B)/2, \quad (3.13) \\ ((\langle\Psi^-| \otimes \mathbb{1}_B) \otimes \mathbb{1}_B)(\alpha|0\rangle_{A_1} + \beta|1\rangle_{A_1}) & \otimes |0,0\rangle_{A_2,B} + |1,1\rangle_{A_2,B})/\sqrt{2} \\ & = iY(\alpha|0\rangle_B + \beta|1\rangle_B)/2, \quad (3.14) \end{aligned}$$

using the Pauli operators X, Y, Z, where

$$Y = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}. \tag{3.15}$$

That is to say, performing the suitable corrections, Bob will deterministically hold the unknown quantum state vector $(\alpha|0\rangle_B + \beta|1\rangle_B)/\sqrt{2}$. The quantum teleportation scheme is complete. Again, neither Alice nor Bob will have to have any classical information about the quantum state in the course of the procedure, and the protocol also does not depend on the state. This is important, since any possibility to learn anything about the unknown input state will disturb this state. Also, all measurement outcomes are equally likely, for the same reason.

3.1.2 All teleportation schemes

This is a puzzling and compelling scheme: The system held by Bob at the end of the protocol is in every way indistinguishable from the input system, even though they have no common past. Also, without sharing entanglement beforehand, the protocol is not possible. But it is also not possible without another ingredient: This is *classical information*: The two bits (and not less) must be transmitted to Bob. This is to be done via a standard classical channel, a phone call, or some transmission line. Both ingredients, entanglement and classical communication, are necessary, and then one is able to perform a task that is classically not possible. Since this scheme is so important, we have a look at it in general terms and make some important remarks. One can see that for any local dimension d, a quantum teleportation scheme can be found. For this to become clear, we need a little bit of preparation.

At the heart of any such scheme is a basis of unitary operators. In the above qubit case, this is constituted by the Paulis $\{X, Y, Z, \mathbb{1}\}$. But more generally, in a quantum system with Hilbert space $\mathbb{C}^d$, we can think of an *orthonormal basis of unitaries*

$$\{U_x : x = 1, \ldots, d^2\} \tag{3.16}$$

that satisfies

$$\operatorname{tr}(U_x U_y^\dagger) = d\delta_{x,y} \tag{3.17}$$

for $x = 1, \ldots, d^2$, where $\delta_{x,y}$ is the Kronecker delta.[1] It is easy to see that the standard qubit Pauli operators do satisfy this for $d = 2$. What is not obvious is that such bases always exist: They do, actually, even though this is very easy to see when d is a prime number and not so easy when it is not. For now, it is sufficient to say that such operators can always be found. Now given a maximally entangled state vector $|\omega\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$, one finds that

$$\{|x\rangle = (\mathbb{1} \otimes U_x)|\omega\rangle : x = 1, \ldots, d^2\} \tag{3.18}$$

constitutes an *orthonormal basis of maximally entangled state vectors*. This is an interesting insight in its own right. By making local basis changes in the second tensor factor, one arrives at orthogonal vectors (in the ordinary sense) which are all maximally entangled. It goes without saying that this immediately generalizes the above setting of

$$(\mathbb{1} \otimes P)(|0, 0\rangle + |1, 1\rangle)/\sqrt{2}, \tag{3.19}$$

for Paulis $P \in \{X, Y, Z, \mathbb{1}\}$.

[1] This orthonormality is actually in the Hilbert-Schmidt scalar product that we will encounter later. To not be overwhelming at this point, we do not go into detail here.

All quantum teleportation schemes: Let $\{U_x \in U(d) : x = 1, \dots, d^2\}$ be an orthonormal basis of unitaries, $\rho_{A_1,C}$ an unknown input state held by Alice and a third party Charlie, and $\omega_{A_2,B}$ a pure maximally entangled state in $\mathbb{C}^d \otimes \mathbb{C}^d$ held by Alice and Bob. Then

$$\sum_x (\mathbb{1}_C \otimes \langle x|_{A_1,A_2} \otimes U_x)(\rho_{A_1,C} \otimes \omega_{A_2,B})(\mathbb{1}_C \otimes |x\rangle_{A_1,A_2} \otimes U_x^\dagger) = \rho_{B,C}. \tag{3.20}$$

Here, for clarity, the tensor factors are given as indices. This may at first sight look overly technical. But it is a cute insight that in fact all possible quantum teleportation schemes are of this form. We will not prove this here. But we will have a look at further important insights.

- As has been said, one does need *entanglement* and one does need *classical communication*. There are no trade-offs. It has to be a maximally entangled state (and not less, then the scheme does not work perfectly any more) and one needs to transmit
$$\log_2(d^2) = 2\log_2(d) \tag{3.21}$$
bits of classical information. In the qubit case, these are two bits.

- We have silently put an important feature in without discussing it, which we do now: The input state initially held by Alice not only does not have to be pure: It can be mixed as well. But it can also be entangled with a third party, say, Charlie. The final state received by Bob, "teleported to Bob", will again be entangled with the same party Charlie. It is really in absolutely every respect that the final state is indistinguishable from the input, including correlations and entanglement with a third party.

- The quantum teleportation scheme does not violate causality. Even though a naive thought might lead to the conclusion that the state is "transported faster than light", this is not so: One does need to send classical bits, and this is possible only with the speed of light or more slowly. Without sending the bits, the state of Bob is actually maximally mixed and contains exactly no infomation about the input. This has to be so, as otherwise, one could devise a Bell's telephone, which we know is not possible.

- As a final remark: If one knows the input state, the rules of the game are changed. The scheme is then called *remote state preparation*. Interestingly, then there are trade-offs in entanglement and classical communication.

3.1.3 A remark on experimental implementations

Unsurprisingly, significant efforts were made to implement this scheme experimentally once it was established. The first key step in this direction was done by the team led by Anton Zeilinger, performing a compelling linear optical experiment that made use of the fact that qubits can be nicely encoded in modes of light in a "dual rail" encoding,

$$|0\rangle \approx |0,1\rangle,\ |1\rangle \approx |1,0\rangle, \tag{3.22}$$

the latter denoting a single excitation in a suitable optical mode. This experiment was highly influential and important, also technologically, and it implemented the teleportation scheme. Or, actually not quite, as it was a scheme that post-selected onto a specific outcome and did not perform the correction. It was still a very important experiment at the time. There was a slightly later experiment that did implement the correction, by a teams led by Jeff Kimble and Eugene Polzik, but in a so-called continuous-variable experiment in which not qubits were encoded, but continuous degrees of freedom. We end this section by giving some literature.

- *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, C. H. Bennett, G. Brassard, C. Crepeau , R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. 70, 1895-1899 (1993).

  This paper introduces the teleportation scheme. At the time, it was a revolutionary thought. Many people think that the first author Charlie Bennett is a natural candidate for the Nobel price for this contributions to quantum physics.

- *Experimental quantum teleportation*, D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature 390, 575-579 (1997).

  A first linear optical implementation of quantum teleportation.

- *Unconditional quantum teleportation*, A. Furusawa, J. L. Sörensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, E. S. Polzik, Science 282, 5389 (1998).

  A first continuous-variable implementation of teleportation.

- *Advances in quantum teleportation*, S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, S. L. Braunstein, Nature Photonics 9, 641 (2015).

  A review on recent developments on teleportation, both conceptually and experimentally.

- *All teleportation and dense coding schemes*, R. F. Werner, quant-ph/0003070

  This work shows that in fact, all teleportation schemes are of the above form.

3.2 Dense coding

3.2.1 Qubit and general schemes

Dense coding is a similar scheme, in fact is makes use of similar ingredients. It is concerned with the coding of classical information into quantum systems. Starting point is the question how many bits we can encode into a quantum system. The answer might be disappointing: One can encode a single bit reliably into a qubit. Of course, state space is bigger, but to reliably perform a measurement, one needs two orthogonal quantum states. That is to say, if qubits are used as elementary carriers of information, one can send one bit per shot, just as if one had used classical systems.

But in some ways, one can do better. If both parties A and B share entanglement beforehand, then they can improve their performance. Let us imagine they initially share

$$(|0,0\rangle + |1,1\rangle)/\sqrt{2}. \tag{3.23}$$

Then Alice can use *two* bits of information and implement, depending on the bit value received, implement one of the unitaries

$$X, iY, Z, \mathbb{1}. \tag{3.24}$$

She sends then the qubit to Bob. Since the resulting set

$$(P \otimes \mathbb{1}_B)(|0,0\rangle + |1,1\rangle)/\sqrt{2} \tag{3.25}$$

constitutes an orthonormal basis of maximally entangled vectors, Bob can reliably distinguish all four of them. Doing so, he receives *two bits of information.* So by sending

- a *single qubit*
- and having a maximally entangled state beforehand

one can send two bits of information. One can argue that in order to establish the entanglement, one needs to send quantum systems as well, which is true, but this can be done beforehand. It still is a task in which entanglement helps to overcome a fundamental limitation. In the same way as above, one can generalize this scheme to arbitrary d: In fact, the very same construction of unitary operator bases features here. One can then send $2\log_2(d)$ bits of information with a single d-dimensional quantum system and a maximally entangled state.

3.2.2 Concluding remarks

While these two protocols, as mentioned above, are somewhat paradigmatic and not really applications, their value can hardly be overestimated. The resource character of entanglement becomes manifest. For qubit teleportation, one can think of the resource count as requiring

- one *ebit* and
- two *bits*

to teleport one *qubit.* The idea of teleportation also plays an important role in quantum error correction, where the variant of teleporting an operation is made use of.