The physics of density matrices (Robert Helling — helling@lmu.de)

1. General remarks

Often (in fact any time we do not consider the whole universe as one big system) we are interested only in subsystems of bigger systems. For example, we want to study an atom in a trap without considering all the 10^{26} other atoms around it or we are interested only in a container of gas and are ignorant of the many degrees of freedom of some "heat bath" it is coupled to. Or we want to understand what is going on in our lab without having to worry what is going on next door.

This is formalised by taking the Hilbert space of the "whole world" to be a tensor product $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ of a Hilbert space $\mathcal{H}_1$for the smaller "system" we are actually interested in and another Hilbert space $\mathcal{H}_2$ of the rest of the world (often called "the environment"). Note well that this is a tensor product ($\otimes$) and not a direct sum ($\oplus$) as one might have assumed, think about it! In these notes, I will always refer to $\mathcal{H}_1$ as "the system", while $\mathcal{H}_2$ is called "the environment" and the combination $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ will be denoted "the whole world".

We will mostly be interested in operators that only act on our system and leave the environment untouched. Those are of the form $\mathcal{O}_1 \otimes id$ while what our colleague does in the lab next door should not affect us and thus is described by operators of the form $id \otimes \mathcal{O}_2$. In addition, however, there can also be interactions between the system and the environment. Those act in both factors of the Hilbert space non-trivially and are thus of the form $\mathcal{O}_1 \otimes \mathcal{O}_2$.

As long as we only make measurements in the system, in $\mathcal{H}_1$ that is, we should have a description that only involves objects (elements, states, operators) of $\mathcal{H}_1$ and not the (possibly much "bigger" $\mathcal{H}$). Doing this, however, one has to be a bit careful: For a general $\Psi \in \mathcal{H}$, there is no $\psi_1 \in \mathcal{H}_1$ that describes the outcome of all measurements in H_1, that is, which fulfils

$$\langle \Psi | \mathcal{O}_1 \otimes id | \Psi \rangle = \langle \psi_1 | \mathcal{O}_1 | \psi_1 \rangle$$

for all operators $\mathcal{O}_1$ on $\mathcal{H}_1$! To describe the state Ψ restricted to the subsystem we need a more general concept of state for $\mathcal{H}_1$ than normalised elements (up to a phase).

To see what is going on, let us expand Ψ in a basis. In order to keep things simple, all Hilbert spaces in these note are finite dimensional. This spares me the worry about convergence issues which are not essential here. However, with some more work, the story also extends to the infinite dimensional case. So taking $(|i_1\rangle)_{i_1 \in I_1}$ to be an orthonormal basis of $\mathcal{H}_1$ and similarly $(|i_2\rangle)_{i_2 \in I_2}$ of $\mathcal{H}_2$, we can write $\Psi = \sum_{i_1,i_2} \psi_{i_1,i_2} |i_1\rangle \otimes |i_2\rangle$. Then

$$\begin{aligned}
\langle \Psi | \mathcal{O}_1 \otimes id | \Psi \rangle &= \sum_{i_1,i_2,j_1,j_2} \bar{\psi}_{j_1,j_2} \psi_{i_1,i_2} \langle j_1 | \mathcal{O}_1 | i_1 \rangle \langle j_2 | i_2 \rangle \\
&= \sum_{i_1,i_2,j_1} \bar{\psi}_{j_1,j_2} \psi_{i_1,i_2} \langle j_1 | \mathcal{O}_1 | i_1 \rangle \\
&= \mathrm{tr}_{\mathcal{H}_1} \gamma \mathcal{O}_1
\end{aligned}$$

if we define the "density matrix"

$$\gamma = \sum_{i_1,i_2,j_1} \bar{\psi}_{j_1,i_2}\psi_{i_1,i_2}|i_1\rangle\langle j_1| = \mathrm{tr}_{\mathcal{H}_2}\left(|\Psi\rangle\langle\Psi|\right).$$

The density matrix γ is an operator on $\mathcal{H}_1$ only and thus we have achieved to write the above expectation value $\mathrm{tr}_{\mathcal{H}_1}\gamma\mathcal{O}_1$ without reference to objects relating to $\mathcal{H}_2$. It is easy to check that γ is a positive operator and $\|\Psi\| = 1$ implies $\mathrm{tr}_{\mathcal{H}_1}\gamma = 1$. We find that the density matrix γ encodes all expectation values for operators acting on $\mathcal{H}_1$.

A density matrix state is a generalisation of a *pure* state given by a normalised element $\psi \in \mathcal{H}_1$ up to multiplication by a phase since $\gamma_\psi = |\psi\rangle\langle\psi|$ also has the properties of a density matrix (that is $\gamma \geq 0$ and $\mathrm{tr}\gamma = 1$). Obviously, it is the density matrices of rank one that correspond to pure states. By the spectral theorem, a general ("mixed") state is a convex linear combination of orthogonal pure states $\gamma = \sum_j \lambda_j|\psi_j\rangle\langle\psi_j|$ with $\sum_j \lambda_j = 1$. The λ_j are the classical probabilities (that is you add the probabilities and not amplitudes, there is no interference) to find the system in state ψ_j. I will come back to this in a later section.

Of course, no one stops us to further subdivide the system into subsystems $\mathcal{H}_1 = \mathcal{H}_{1'}\otimes\mathcal{H}_{1''}$. And as long as we only measure observables $\mathcal{O}_{1'}$ we can restrict ourselves to a mixed state on $\mathcal{H}_{1'}$ given by the further reduced density matrix $\gamma' = \mathrm{tr}_{\mathcal{H}_{1''}}\gamma$. On the other hand, we should envision the possibility that what we thought of as the whole world $\mathcal{H}$ is only a subsystem of an even bigger $\tilde{\mathcal{H}} = \mathcal{H}\otimes\mathcal{H}'$ since there are further degrees of freedom that we have not considered so far. Consequently, we should allow also mixed states described by a general density matrix for $\mathcal{H}$. Such arguments lead us to conclude that for any Hilbert space it is natural to consider the set of density matrices as the set of states and the pure states given by normalised wave functions only as a special subclass of those having rank one.

Having generalised our idea of what constitutes a state, we might worry that there are further generalisations ahead. In a sense, however, one can see that this is not the case and density matrices are the most general states: If we abstractly define a state as a map $\omega\colon \{operators\} \to \mathbb{C}$ that maps operators to their expectation values (after all that's what characterises a state: The results of all possible measurements) then it is natural to require the following: ω is linear, that is the expectation value of the operator $2\mathcal{O}$ is twice the expectation value of $\mathcal{O}$ and the expectation value of $\mathcal{O}_1 + \mathcal{O}_2$ is the expectation value of $\mathcal{O}_1$ plus the expectation value of $\mathcal{O}_2$. This means that states ω are elements of the dual space of the space of operators. For bounded operators (which are the nice class anyway, and remember, in the finite dimensional case boundedness is automatic) this means ω can be viewed as taking the trace against a trace class operator, that is ω corresponds to a γ which is trace class and for an operator $\mathcal{O}$ the expectation value is $\omega(\mathcal{O}) = \mathrm{tr}\gamma\mathcal{O}$. Furthermore, the identity operator should have expectation value 1 which implies $\omega(id) = \mathrm{tr}\gamma id = \mathrm{tr}\gamma = 1$. Finally (this is slightly less obvious), positive operators $\mathcal{O} \geq 0$ should have positive expectation values which implies γ to be positive. Therefore, we see that the density matrices are all states being defined as normalised positive linear functionals on the bounded operators.

As a last remark of this general introductory section, I would like to point out that there is an approach to quantum theory where one starts out without an a priori Hilbert space but with just an abstract (C*) algebra of observables (defined in terms of their commutation relations). In that approach, a state is a linear functional ω as above (normalised, positive). From such a state, one can then construct the Hilbert space as a representation of the observable algebra in such a way that ω corresponds to a vector in that Hilbert space. In this construction due to Gelfand, Naimark and Segal (GNS), the representation is irreducible exactly if the state ω is pure, that is it cannot be written as a proper convex combination of two other states.

2. Mixed states versus superpositions

Given two orthonormal vectors $\psi_1, \psi_2 \in \mathcal{H}$. We have concluded that the mixed state $\gamma_m := \frac{1}{2}|\psi_1\rangle\langle\psi_1| + \frac{1}{2}|\psi_2\rangle\langle\psi_2|$ describes a system which is with probability 50% in the state ψ_1 and with probability 50% in the state ψ_2. *Nevertheless, this must not be confused with the superposition* $\psi_s = \frac{1}{\sqrt{2}}(\psi_1 + \psi_2)$*!* When we make a measurement to see if the system is in the state ψ_1 we can do this using the projector $|\psi_1\rangle\langle\psi_1|$ as our observable. Both γ_m and ψ_s give 0 and 1 with probability 50% and similarly for ψ_2. However, the two states differ when we measure other observables.

The difference between the two states γ_m and ψ_s is that for the mixed state we first take ψ_1 and ψ_2 modulo a phase and then put them together in a probabilistic way whereas for ψ_s we add them with a definite relative phase and only after the combination mod out by an overall phase.

In formulas, this can be seen when we write the density matrix for ψ_s in its components:

$$\begin{aligned}\gamma_s &= |\psi_s\rangle\langle\psi_s| \\ &= \frac{1}{2}(|\psi_1\rangle + |\psi_2\rangle)(\langle\psi_1| + \langle\psi_2|) \\ &= \frac{1}{2}(|\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2| + |\psi_1\rangle\langle\psi_2| + |\psi_2\rangle\langle\psi_1|).\end{aligned}$$

Or as matrices in the basis $\{\psi_1, \psi_2\}$:

$$\gamma_m = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \qquad \gamma_s = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}.$$

We see, as expected γ_m has rank two while γ_s has rank one (it is pure after all). This representation reveals which observable differentiates between the two states: We can take the Pauli matrix $\sigma_x = \frac{1}{2}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$. This is hermitian with eigenvalues $\pm\frac{1}{2}$ (remember, those are the possible outcomes of measurements of σ_x). We compute the two expectation values

$$\mathrm{tr}\gamma_m\sigma_x = \mathrm{tr}\frac{1}{4}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = 0 \qquad \mathrm{tr}\gamma_s\sigma_x = \mathrm{tr}\frac{1}{4}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix} = \frac{1}{2}.$$

If the system is in the state γ_m, measuring σ_x gives half of the time the result $-\frac{1}{2}$ while the other half of the measurements gives $+\frac{1}{2}$. In the superposition γ_s however, measuring σ_x always yields the result $+\frac{1}{2}$, not surprising given that ψ_s is an eigenvector of σ_x.

3. Entropies

We have seen that pure states correspond to rank one density matrices whereas mixed states have higher rank. In addition to this binary criterion for pureness there are a number of continuous quantities assessing the "pureness" of a state. For example, since γ is positive and has trace one, $\mathrm{tr}\gamma^2$ is one only for pure states while it is less than one for mixed states as can most easily seen from the spectral decomposition. Similarly, the α-entropy is defined for $\alpha > 0$ and $\alpha \neq 1$ as $S_\alpha = \frac{1}{1-\alpha} \log \mathrm{tr}\gamma^\alpha$. The limiting case of this is the von Neumann entropy

$$S = \lim_{\alpha \to 1} S_\alpha = -\mathrm{tr}\gamma \log \gamma$$

known form statistical physics and thermodynamics. All these entropies vanish for pure states and are positive for mixed states. For example if γ is the complete mixture between N states, that is it is $1/N$ times a projector on an N-dimensional subspace, all α-entropies are $\log N$.

Note that all these measures are mathematical quantities assessing the mixedness of a state γ. They do not correspond to a physical measurement in the sense that there is no operator $\mathcal{O}$ such that for all γ the entropy S_α is the expectation value of $\mathcal{O}$.

In addition, the entropies depend on the choice of subsystem. Above we have seen the example of the world being in a pure state (thus having vanishing entropy) while the subsystem is in a mixed state with positive entropy. In fact, given the dimension of the environment Hilbert space $\mathcal{H}_2$ is big enough, any mixed state γ on $\mathcal{H}_1$ can be purified to a pure state on $\mathcal{H}$. If in a spectral decomposition $\gamma = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|$ and $(|j\rangle)_{j\in J}$ is an orthonormal basis of $\mathcal{H}_2$ then an example of a pure state reducing to γ is $\sum_j \sqrt{\lambda_j}|\psi_j\rangle \otimes |j\rangle$.

On the other hand, it is also possible (and in fact common) that the entropy of the whole world is bigger than the entropy a subsystem. For example a pure state on $\mathcal{H}_1$ can be the reduction of a mixed state on $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. For example, given a mixed state γ_2 on $\mathcal{H}_2$, ψ_1 is the pure reduction of the mixed state $|\psi_1\rangle\langle\psi_1| \otimes \gamma_2$ on $\mathcal{H}$.

For our discussion, we only needed that $\mathcal{H}_1$ is a tensor factor of a bigger Hilbert space $\mathcal{H}$. It is possible that $\mathcal{H}_1$ corresponds to a subset of a particles but this is not necessary. Another characterisation would be to start form a subset of operators and declare only those as observable while one is ignorant of the remaining ones. Now, one can consider a tensor factor $\mathcal{H}_1$ of the total Hilbert space such that all observable operators decompose as $\mathcal{O}_1 \otimes id$ upon writing $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. Then one can consider the entropy of the state reduced to $\mathcal{H}_1$ as the entropy with regard to the choice of observables. An example of this procedure is the relation of thermodynamics to statistical physics (quantum or classical): In thermodynamics, one observes only macroscopic properties of a system like pressure, energy, chemical potential, magnetisation etc. while being ignorant of the microscopic

degrees of freedom like the positions of individual molecules. Therefore one typically observes a mixed state macroscopically (that is on $\mathcal{H}_1$) although microscopically (on $\mathcal{H}$) the system is in a pure state. Therefore, saying a state is pure or mixed is always relative to a fixed Hilbert space. Allowing additional observables and a larger Hilbert space of so far ignored degrees of freedom can change the nature of the state in both directions.

4. Time evolution

As long as the system $\mathcal{H}_1$ and the environment are decoupled one can ignore the environment for the time evolution. This means, if the Hamiltonian of the whole world has the form $H = H_1 \otimes id + id \otimes H_2$ leading to a unitary time evolution operator $U(t) = U_1(t) \otimes U_2(t)$, the reduced density matrix γ follows a Heisenberg equation $i\partial_t \gamma_t = [H, \gamma_t]$ or in the integrated version $\gamma_t = U_1(t)\gamma_0 U_1(t)^{-1}$.

For any unitary U, it follows from the spectral theorem that for any function f one has $f(U\gamma U^{-1}) = Uf(\gamma)U^{-1}$. Cyclicity of the trace then implies that the entropies do not change over time as long as the system and the environment are decoupled as above. Especially, no system left to its own will change over time from a pure state to a mixed state or vice versa.

Therefore, to make an experiment with the subsystem in a specific pure state starting from a mixed state, we cannot do this acting only on the system and not on the environment. In practice, in the preparation, one filters out all states but those in a one dimensional subspace. For example, to produce a beam of electrons with spin pointing up one uses a Stern-Gerlach type experiments which separates the two spin states of the electron and then blocks the beam with the spin pointing down. More abstractly, one measures the spin and discards all but one eigenstate. Discarding, however is not a unitary operation with respect to the spin Hilbert space of the electron. To get rid of the electrons with spin down, one has to let them interact with the environment. Thus our assumption above about the form of the time evolution not mixing system and environment do not hold for this filtering stage and we can turn an electron spin which was mixed originally into a pure spin state.

Let us investigate an example of time evolution, a simplified version of the Aharonov-Bohm effect. We use this to demonstrate that the lacking phase relation for mixed states mentioned above leads to classical behaviour of a quantum system.

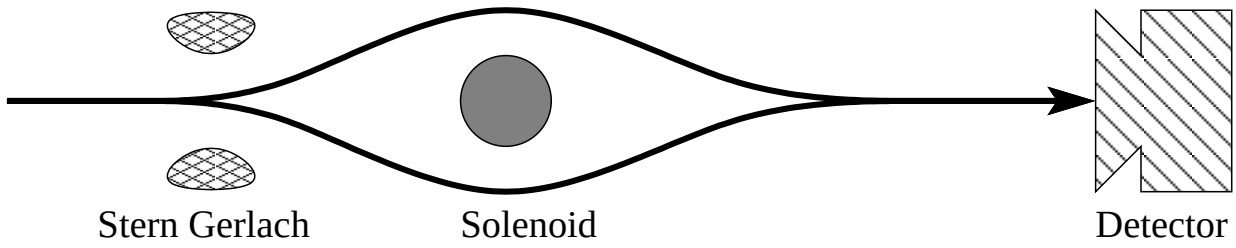

Fig. 1: An Aharonov-Bohm type experiment

We take our two state system of section 2, for example thinking of it as spin up and down. First, by an inhomogeneous field à la Stern-Gerlach, we split up the two states, one goes up and the other goes down. The two states pass a solenoid with a magnetic field on two different sides. This has the effect of multiplying ψ_1 by a phase $e^{i\phi}$ proportional to the magnetic field and ψ_2 by the opposite phase $e^{-i\phi}$. This time evolution is thus given by the unitary matrix $U = \begin{pmatrix} e^{i\phi} & \\ & e^{-i\phi} \end{pmatrix}$. Finally, the two beams are combined again and the detector clicks according to the sum of the amplitudes of the two beams that is, the observable is the projector onto $\psi_1 + \psi_2$ that is $\mathcal{O} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. The initial state shall be as in section 2, we have $\gamma_{m/s} = \frac{1}{2} \begin{pmatrix} 1 & \zeta \\ \zeta & 1 \end{pmatrix}$ with $\zeta = 1$ for the superposition of ψ_1 and ψ_2 and $\zeta = 0$ for the mixed state. Hence, we compute for the clicking probability of the detector

$$\begin{aligned}
\langle \mathcal{O} \rangle &= \operatorname{tr}(U \gamma_{m/s} U^{-1} \mathcal{O}) \\
&= \operatorname{tr}\left[\begin{pmatrix} e^{i\phi} & \\ & e^{-i\phi} \end{pmatrix} \frac{1}{2} \begin{pmatrix} 1 & \zeta \\ \zeta & 1 \end{pmatrix} \begin{pmatrix} e^{-i\phi} & \\ & e^{i\phi} \end{pmatrix} \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right] \\
&= \frac{1}{2}(1 + \zeta \cos\phi) \\
&= \begin{cases} \frac{1}{2} & \text{mixed} \\ \cos^2 \phi & \text{superposition} \end{cases}
\end{aligned}$$

We find that in the superposition state the clicking rate is modulated by the phase due to the magnetic field in the solenoid while the clicking is not affected by a phase shift in the mixed state. There is no interference between the particles taking the upper path and the particles taking the lower in the mixed state. In this respect, the mixed state behaves classically.

5. An application: Quantum cryptography

In this application, Alice wants to transmit a message to Bob. However, they want to make sure that Eve, an eavesdropper, cannot get the information as well. Let us assume the message is a single bit. The first idea for Alice and Bob is to share an additional random bit. For example, Alice could have two pairs of socks, a white one and a red one curled up as pairs in her drawer. In the morning, before switching on the lights, she reaches in the drawer and picks a random pair. She takes one sock of the pair in an envelope and sends it to Bob. Then, later that day, she figures out what the message is. Then she looks at the single sock that is left over from the pair she picked in the morning. If it is red, she flips the message bit but she keeps the bit in tact if the sock is white. This now possibly modified message bit she announces with a megaphone so everybody including Bob and Eve can hear it. Since Bob has received the sock by mail he knows that in case he has received a red sock he has to flip the bit he heard Alice announce through the megaphone and if he received a white sock he can take the message literally.

If Eve does not know the colour of the sock that was mailed to Bob she has no use of the

message she heard when Alice announced it since she does not know if she has to flip the bit to get the true message or not.

Of course, this protocol is too simple since if Eve cannot access the mail there is no point for cryptography, Alice could just mail the message to Bob. We want, however, to have a cryptographic protocol that even works if Eve can read the mail for example if she is the post-woman. This can be done if instead of mailing socks Alice mails quantum states.

We have to use only a slightly more complicated set-up as in the previous sections since now we have three parties: Alice, Bob, and Eve each have their own Hilbert space and the total Hilbert space is a tensor product of three factors $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$. It is sufficient to take $\mathcal{H}_A$ and $\mathcal{H}_B$ to be two dimensional (a "qubit"). Now, instead of drawing a pair of socks, Alice prepares two entangled qubits, that is, she produces the pure state $\psi = \frac{1}{\sqrt{2}}(|\psi_1\rangle_A \otimes |\psi_1\rangle_B + |\psi_2\rangle_A \otimes |\psi_2\rangle_B) \in \mathcal{H}_A \otimes \mathcal{H}_B$ the B part she sends off to Bob by mail.

Then she makes a measurement of the operator $\mathcal{O} = \sigma_z = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ in $\mathcal{H}_A$, her remaining qubit. She will get the result $\pm\frac{1}{2}$, each with 50% probability. If Bob measures the same $\mathcal{O}$ but now on his qubit in $\mathcal{H}_B$ he also gets $\pm\frac{1}{2}$ each with probability 50%. The important thing however is, that both will always get the same result: We can check the correlation by computing $\langle(\sigma \otimes id)(id \otimes \sigma)\rangle_\psi = \langle \sigma \otimes \sigma \rangle_\psi$ in $\mathcal{H}_A \otimes H_B$:

$$\begin{aligned}
\langle \sigma \otimes \sigma \rangle_\psi &= \langle \psi | \sigma \otimes \sigma | \psi \rangle \\
&= \frac{1}{2}\Big(\langle \psi_1 | \sigma | \psi_1 \rangle_A \langle \psi_1 | \sigma | \psi_1 \rangle_B \\
&\quad + \langle \psi_1 | \sigma | \psi_2 \rangle_A \langle \psi_1 | \sigma | \psi_2 \rangle_B \\
&\quad + \langle \psi_2 | \sigma | \psi_1 \rangle_A \langle \psi_2 | \sigma | \psi_1 \rangle_B \\
&\quad + \langle \psi_2 | \sigma | \psi_2 \rangle_A \langle \psi_2 | \sigma | \psi_2 \rangle_B \Big) \\
&= \frac{1}{2}\left(\frac{1}{4}\frac{1}{4} + 0 + 0 + \frac{1}{4}\frac{1}{4} \right) = \frac{1}{4}
\end{aligned} \quad .$$

The same would happen if both measured instead $\mathcal{O} = \sigma_x$ or $\mathcal{O} = \sigma_y = \frac{1}{2}\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$ (check it!). Thus, in this quantum protocol they could proceed as with the socks both flipping the message bit when measuring $\frac{1}{2}$ and not flipping it when measuring $-\frac{1}{2}$.

The difference to the classical protocol with socks is that the quantum protocol is tamper proof: Eve has no chance to intercept the mail and and look at the qubit for Bob without altering the state shared by Alice and Bob in $\mathcal{H}_A \otimes \mathcal{H}_B$. It can be shown that after doing something with the qubit for Bob (applying a non-diagonal unitary transformation in $\mathcal{H}_B \otimes \mathcal{H}_E$) such that afterwards the state in $\mathcal{H}_E$ has some information about Bob's qubit then the combined state of Alice and Bob in $\mathcal{H}_A \otimes \mathcal{H}_B$ is mixed and the von Neumann entropy of the density matrix in $\mathcal{H}_A \otimes \mathcal{H}_B$ is a measure of the information Eve has obtained.

As an example, let us assume that Eve "makes a copy" of Bob's qubit. That is she starts out with $\psi_1 \in \mathcal{H}_E$ say and takes Bob's qubit $\psi_B \in \mathcal{H}_B$ into the tensor product state

$\psi_B \otimes \psi_B \in \mathcal{H}_B \otimes \mathcal{H}_E$ (convince yourself that this can be done by a unitary transformation!). The threesome holds now the state $\psi_{ABE} = \frac{1}{\sqrt{2}}(|\psi_1\rangle_A \otimes |\psi_1\rangle_B \otimes |\psi_1\rangle_E + |\psi_2\rangle_A \otimes |\psi_2\rangle_B \otimes |\psi_2\rangle_E) \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$.

When Alice and Bob now measure $\mathcal{O} = \sigma_z$ Eve can measure this operator as well on her qubit and she will get the same result as the two. It looks like we have gained nothing compared to the sock protocol. The crucial difference however is that Alice and Bob can detect Eve's tampering: When restricting ψ_{ABE} to $\mathcal{H}_A \otimes \mathcal{H}_B$ it becomes mixed. It is given by the density matrix $\gamma_{AB} = \frac{1}{2}(|\psi_1\rangle_A \otimes |\psi_1\rangle_B \langle\psi_1|_A \otimes \langle\psi_1|_B + |\psi_2\rangle_A \otimes |\psi_2\rangle_B \langle\psi_2|_A \otimes \langle\psi_2|_B)$. Alice and Bob can now detect the tamper by both measuring $\mathcal{O} = \sigma_x$ and then announcing the result using megaphones. They will detect that the perfect correlation between their measurements is gone as soon as Eve has obtained her copy (check this!).

Of course, once Alice and Bob do the measurement to detect Eve's interference they cannot use the pair of qubits anymore to encode the message. The way out for Alice and Bob is not to share a single pair of qubits but to share N such pairs. After Bob has obtained his N qubits, Alice and Bob pick he same random subsample of the qubits and measure the correlation of their results when measuring some of the σ-matrices as observables. If Eve has not interfered, they will find total correlation, otherwise they will get differing results. The remaining pairs can then be used to encode a message. Since Eve does not know beforehand which pairs will be used for message encoding and which pairs will be checked for tampering she must not interfere at all if she does not want to be detected. In fact, one can show, that N can be picked large enough such that the probability of Eve obtaining information about the message and not being detected is arbitrarily small.