Notes on Classical & Quantum Error-Correcting Codes

March 27, 2018

P. Ramond

Lecture 5: It's Quantum Mechanics!

Measurement in Quantum Mechanics is pretty tricky because of the role of the observer. This lecture introduces the basic concepts where the observer is viewed as separate from the system whose properties are being measured, all the way to Everett's contribution where the observer is part and parcel of the whole system.

Bauer & London

In June 1939 at the Sorbonne in Paris, Fritz London and Edmund Bauer gave a set of wonderful lectures entitled *The Theory of Observation in Quantum Mechanics*. They are succinct and to the point; the following is a modern rendition. It begins with pronouncements by the founding fathers as well as observations.

• Max Born: *"Even though the notion of particles might be determined only by probabilities these very probabilities evolve in accordance with a causal law."*

• Heisenberg: *"It is the act of measurement which introduces the element of uncertainty."*

• Schrödinger's equation yields causal connections, yet $|\Psi|^2$ is a probability dis-

tribution, and probabilities implies partial knowledge. They are interpreted as probabilities of the outcome of measurements, and are only potential probabilities.

If the wave function has an objective character, as in physical optics, it represents a complete image of the object. There should be no uncertainty: where do probabilities come from?

Pure States

A quantum mechanical state described by a normalized ket $|\,\psi\,\rangle$ which lives in a Hilbert space $\mathcal{H}$ is called a pure state. One can form its density matrix, which they call the *statistical matrix*,

$$\rho \equiv |\,\psi\,\rangle\langle\,\psi\,|.$$

Its trace properties are maintained by unitary evolution $\mathcal{U}$, since

$$|\,\psi\,\rangle \quad\longrightarrow\quad |\,\psi'\,\rangle = \mathcal{U}|\,\psi\,\rangle, \quad \rho \quad\longrightarrow\quad \rho' = \mathcal{U}\,\rho\,\mathcal{U}^\dagger.$$

Since $|\,\psi\,\rangle$ is normalized, its trace is unity, $\mathrm{Tr}\,\rho = 1$. In addition,

$$\rho^2 = \rho \quad\longrightarrow\quad \mathrm{Tr}\,\rho^2 = 1.$$

indicating that for a pure state, ρ is a projection operator. This is the hallmark of pure states.

The wavefunction can always be expressed as a linear combination of states $|\,a\,\rangle$ which form a complete orthonormal basis in $\mathcal{H}$,

$$|\,\psi\,\rangle = \sum_a \psi_a |\,a\,\rangle.$$

If the basis states are eigenstates of the Hamiltonian, assuming non-degeneracy for simplicity,

$$H|\,a\,\rangle = E_a|\,a\,\rangle,$$

and the absolute square of the coefficient $|\psi_a|^2$ is the probability of finding the state with energy E_a.

We can express the expectation value of any operator F in this pure state as,

$$\langle F\rangle_{\mathrm{pure}} = \langle\,\psi\,|\,F\,|\,\psi\,\rangle = \sum_{a,b} \psi_a^*\psi_b \langle\,a\,|\,F\,|\,b\,\rangle.$$

Mixtures

Bauer and London consider a mixture of pure states, $|\, a_i \,\rangle$, with "concentrations" p_i, and $\sum_i p_i = 1$.

The "value" of any operator in the mixture is naturally given by the average of its value in the pure state $|\, a_i \,\rangle$, weighted by the concentration p_i, the statistical sum,

$$\langle F \rangle_{\rm mixture} = \sum_i p_i \langle\, a_i \,|\, F \,|\, a_i \,\rangle.$$

If F is any operator that commutes with the Hamiltonian, for two different states $a \neq b$,

$$0 = \langle\, a \,|[F, H]|\, b \,\rangle = (E_b - E_a) \langle\, a \,|F|\, b \,\rangle,$$

then $\langle\, a \,|F|\, b \,\rangle = 0$ since $E_b \neq E_a$. It follows that

$$\langle F \rangle_{\rm pure} = \langle F \rangle_{\rm mixture},$$

with $p_i = |\psi_i|^2$.

On the other hand, if $[\, F \,,\, H \,] \neq 0$,

$$\langle\, a \,|\, F \,|\, b \,\rangle = F_{ab} \neq \delta_{ab} F_a,$$

and, setting $\psi_a = \sqrt{p_a} e^{i\alpha_a}$,

$$\langle\, F \,\rangle_{\rm pure} = \sum_{a,b} \sqrt{p_a p_b} e^{i(\alpha_a - \alpha_b)} F_{ab}, \qquad \langle\, F \,\rangle_{\rm mixture} = \sum_a p_a F_{aa},$$

showing that they are different.

The pure state value includes the phases while the mixture value does not! Information has been lost by considering the mixture over the pure state, which explains why probabilities appear. Mixtures are different from pure states, although mixture and pure state values can be made to coincide by further averaging over the phases.

The density matrix for a mixture is defined by,

$$\rho_{\rm mixture} \equiv \sum_i p_i |\, a_i \,\rangle \langle\, a_i \,|;$$

it also has unit trace,

$$\mathrm{Tr}(\rho_{\rm mixture}) = \sum_i p_i \langle\, a_i \,|\, a_i \,\rangle = \sum_i p_i = 1,$$

but it is not a projection operator,

$$\rho^2_{\rm mixture} = \sum_{ij} p_i p_j |\, a_i \,\rangle\langle\, a_i \,|\, b_j \,\rangle\langle\, b_j \,| = \sum_i p_i^2 |\, a_i \,\rangle\langle\, a_i \,| \neq \rho_{\rm mixture}.$$

It follows that

$$\rho^2_{\rm mixture} - \rho_{\rm mixture} = \sum_i p_i(p_i - 1) |\, a_i \,\rangle\langle\, a_i \,|,$$

and the coefficients are all negative, so that in any state the operator $\rho^2 - \rho$ is semi-definite. In particular,

$$\mathrm{Tr}(\rho^2_{\rm mixture}) - \mathrm{Tr}(\rho_{\rm mixture}) \;\leq\; 0,$$

with the equality holding only for a pure state. The expectation value of any operator F is written as,

$$\langle\, F \,\rangle = \mathrm{Tr}(\rho F).$$

for any (pure or mixture) density matrix ρ.

Given two density matrices ρ_A and ρ_B, define

$$\rho_{AB} = \alpha\rho_A + \beta\rho_B,$$

where α, $\beta \geq 0$, and $\alpha + \beta = 1$. Then

$$\begin{aligned} \rho^2_{AB} &= \alpha^2\rho_A^2 + \beta^2\rho_B^2 + \alpha\beta(\rho_A\rho_B + \rho_B\rho_A) \\ &= \alpha\rho_A^2 + \beta\rho_B^2 - \alpha\beta(\rho_A - \rho_B)^2, \end{aligned}$$

using $\alpha + \beta = 1$. It follows that

$$\rho_{AB} - \rho^2_{AB} = \alpha(\rho_A - \rho_A^2) + \beta(\rho_B - \rho_B^2) + \alpha\beta(\rho_A - \rho_B)^2.$$

Since $\rho_{A,B}$ are density matrices, the right-hand side of this equation has positive or zero eigenvalues: ρ_{AB} is a density matrix.

If ρ_{AB} represents a pure state, the right-hand side has only zero eigenvalues, so that $\rho_A = \rho_B = \rho_{AB}$. It is not possible to represent a pure case in terms of mixtures. If all three, ρ_{AB} and $\rho_{A,B}$ represent pure states, then $\rho_{AB} = \rho_A = \rho_B$: they form a convex set. If ρ_A and ρ_B represent pure states, then

$$\rho_{AB} - \rho^2_{AB} = \alpha\beta(\rho_A - \rho_B)^2,$$

has only positive eigenvalues and ρ_{AB} represents a mixture, unless $\rho_A = \rho_B$.

Introduce the states

$$|\,\tilde{a}\,\rangle_B \equiv \sum_b \omega_{ab} |\,b\,\rangle_B.$$

Their inner product is the density matrix for the A-system

$${}_B\langle\,\tilde{a}\,|\tilde{a}'\rangle_B = \sum_b \omega^*_{ab}\omega_{a'b} = \rho_{A\,aa'}.$$

When the density matrix is expressed in its diagonal canonical form

$$\rho_A = \sum_a p_a |\,a\,\rangle_{A\,A}\langle\,a\,|,$$

we get

$${}_B\langle\,a\,|a'\rangle_B = p_a\delta_{aa'}.$$

In this new basis, the compound state becomes

$$|\,\Psi\,\rangle_{AB} = \sum_a \sqrt{p_a}|\,a\,\rangle_A \otimes |\,a\,\rangle_B$$

where,

$$|\,a\,\rangle_B = \frac{1}{\sqrt{p_a}}|\,\tilde{a}\,\rangle_B.$$

This is the Schmidt decomposition of the compound state written in terms of orthonormal states in both Hilbert spaces.

It allows us to find an alternate expressions for the density matrices. Since

$$\mathrm{Tr}_B\mathcal{O} = \sum_a {}_B\langle\,a\,|\mathcal{O}|\,a\,\rangle_B,$$

we find

$$\rho_A = \mathrm{Tr}_B\big[|\,\Psi^{AB}\,\rangle\langle\,\Psi^{AB}\,|\big], \qquad \rho_B = \mathrm{Tr}_A\big[|\,\Psi^{AB}\,\rangle\langle\,\Psi^{AB}\,|\big],$$

using the orthonormality of the bases. Note that the same non-zero probabilities p_a appears in both expressions although the A and B systems will differ in their number of zero eigenvalues.

The"information" contained in a quantum state with density matrix ρ is given by the von Neumann entropy,

$$S(\rho) = -\mathrm{Tr}[\rho\log\rho].$$

- The entropy of a pure state for which ρ has one non-zero eigenvalue vanishes.

- The entropy of a compound state ρ_{AB} satisfies the subadditivity constraint,

$$S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B),$$

which states that the information in the compound state is less than the total input information: information has been lost in forming the compound state.

Applying these to the Schmidt decomposition, we find,

$$S(\rho_{AB}) = 0 \quad \longrightarrow \quad S(\rho_A) = S(\rho_B) \geq 0.$$

An important application is the association of a pure state to an impure state in a process called *purification*. Given a mixture density matrix ρ_A, with ket $|\,\psi_A\,\rangle$, we adjoin another Hilbert space $\mathcal{H}_B$ and form the pure state,

$$|\,\psi^{AB}\,\rangle = |\,\psi^A\,\rangle \otimes |\,\phi^B\,\rangle, \qquad \rho^{AB} = \rho^A \otimes |\,\phi^B\,\rangle\langle\,\phi^B\,|,$$

where $|\,\phi^B\,\rangle$ is any normalized state in $\mathcal{H}_B$.

The original density matrix is the partial trace over B of the AB density matrix

$$\rho_A = \mathrm{Tr}_B\big[\rho_{AB}\big] = \mathrm{Tr}_B\big[|\,\psi^{AB}\,\rangle\langle\,\psi^{AB}\,|\big],$$

It looks like a cheap trick (it is!), but it allows for different ways of expressing the physics of the A system.

Quantum Weirdness of Measurements

Consider atoms with spin eigenvalues $\pm\frac{1}{2}$ in some direction, and eigenkets $|\,u_\pm\,\rangle$. Take the atom in the pure state $|\,\psi\,\rangle = |\,u_+\,\rangle$ with spin one-half in the z direction. In terms of possibilities $p_+ = 1$, $p_- = 0$.

The same state can be expressed as a linear combination of eigenstates $|\,u'_\pm\,\rangle$ in the (θ, ϕ) direction,

$$|\,\psi\,\rangle = |\,u_+\,\rangle = e^{i\phi/2}\cos\frac{\theta}{2}|\,u'_+\,\rangle + e^{-i\phi/2}\sin\frac{\theta}{2}|\,u'_-\,\rangle$$

In the z direction, we have , while along the (θ, ϕ) direction,

$$p'_+ = \cos^2\frac{\theta}{2}, \qquad p'_- = \sin^2\frac{\theta}{2}$$

So if we consider a large ensemble of atoms, this combination describes 100% of the atoms with spin plus one-half in the z-direction, while we find $(\cos^2\frac{\theta}{2})\%$ with spin plus one-half and $(\sin^2\frac{\theta}{2})\%$ with spin minus one-half along the (θ, ϕ) direction. If we were to measure the spin in the (θ', ϕ') direction, we would find $(\cos^2\frac{\theta'}{2})\%$ with spin plus one-half.

We have several outcomes for the same pure state $|\,\psi\,\rangle$, depending on the setting of the measuring apparatus:

$$\begin{aligned} &\text{spin along } \ z: \qquad p_+ = 1, \qquad\qquad p_- = 0, \\ &\text{spin along } \ (\theta,\phi): p'_+ = \cos^2\frac{\theta}{2}, \qquad p'_- = \sin^2\frac{\theta}{2}. \end{aligned}$$

How can we make sense of this situation? It depends how we measure so that the answer is the intervention of the measuring observer.

Statistics of a System Composed of Two Subsystems

"What happens when we bring in contact two systems which were originally in pure states and subsequently separate?" On the surface nothing much since a pure state evolves in time to another pure state according the Schrödinger's equation, but ... .

Consider two pure systems, A and B, with wavefunctions $|\,\psi\,\rangle_A$ and $|\,\chi\,\rangle_B$, expanded in terms of their own orthogonal bases,

$$|\,\psi\,\rangle_A = \sum_a \psi_a |\,a\,\rangle_A, \qquad |\,\chi\,\rangle_B = \sum_b \chi_b |\,b\,\rangle_B$$

Each has its own Hamiltonian, with $H = H_A + H_B$, and the two systems evolve independently, with a common wavefunction,

$$|\,\Psi\,\rangle_{AB} = |\,\psi\,\rangle_A \otimes |\,\chi\,\rangle_B = \sum_{a,b} \psi_a\chi_b |\,a\,\rangle_A \otimes |\,b\,\rangle_B.$$

Let the two systems interact with one another for a short time. The Hamiltonian is now $H = H_A + H_B + H_{AB}$. The resulting common wavefunction is a pure state for the whole $A + B$ system. It can be expanded as

$$|\,\Psi\,\rangle_{AB} = \sum_{a,b} \omega_{ab} |\,a\,\rangle_A \otimes |\,b\,\rangle_B$$

where the coefficients $\omega_{ab} \neq \psi_a\chi_b$.

Assume that the two systems have separated, and we want to determine the value of some operator F_A of the form

$$F_A = \sum_{a,a'} f_{aa'} |\,a\,\rangle_A\,{}_A\langle\,a'\,|,$$

which lives in the Hilbert state $\mathcal{H}_A$. Using the orthogonality of the $|\,a\,\rangle_A$ and $|\,b\,\rangle_B$ bases,

$$ {}_{AB}\langle\,\Psi\,|F_A|\,\Psi\,\rangle_{AB} = \sum_{aa'} f_{aa'} \sum_b \omega^*_{ab}\omega_{a'b} \;\equiv\; \mathrm{Tr}(\rho_A F_A), $$

defining the density matrix elements of system A as

$$ (\rho_A)_{aa'} = \sum_b \omega^*_{ab}\omega_{a'b}. $$

Its trace is equal to one, but it is not a projection operator. We can express it in terms of hatted normalized wavefunctions as

$$ (\rho_A)_{aa'} = \sum_b p_b\, \hat{\omega}^*_{ab}\hat{\omega}_{a'b}, \qquad p_b = \sum_a |\omega_{ab}|^2, \quad \sum_b p_b = 1. $$

A similar reasoning applied to an operator in the B system yields the density matrix,

$$ (\rho_B)_{bb'} = \sum_a p_a\, \hat{\omega}^*_{ab}\hat{\omega}_{ab'}, \qquad p_a = \sum_b |\omega_{ab}|^2, \quad \sum_a p_a = 1. $$

Both density matrices describe mixtures.

When two pure states interact, the resulting wavefunction is a pure state (unitary evolution maps pure states into pure states), but the value of any operator that pertains only to system A or B variables is determined probalistically, since information has been lost by not sampling the full Hilbert space (only sum over a or over b but not both). Whenever a system A gets in contact with another B, one loses some knowledge of the original system A. That is just the way it is in quantum land!

The pure state density matrix,

$$ \rho_{AB} = |\,\Psi\,\rangle_{AB\,AB}\langle\,\Psi\,|, $$

and the partial density matrices ρ_A and ρ_B are not unitarily related. True, one can go from ρ_{AB} to either ρ_A or ρ_B by taking partial sums, it is not possible to go backwards.

This analysis applies to the measurement process, where system A is the object system whose properties are to be measured, and system B describes a measuring apparatus.

Let system B be the pointer system, and assume one of its variables takes a number of eigenvalues g_0, g_1, ..., g_i, ..., g_N, corresponding to eigenvectors $|\,i\,\rangle$. Initially the pointer state is set at $|\,0\,\rangle_B$ with eigenvalue g_0, so that

$$|\,\Psi\,\rangle_{AB} = \sum_a \psi_a |\,a\,\rangle_A \otimes |\,0\,\rangle_B.$$

As a result of interaction between the two systems, the wavefunction becomes entangled as,

$$|\,\Psi\,\rangle_{AB} = \sum_{a,i} \omega_{a\,i} |\,a\,\rangle_A \otimes |\,i\,\rangle_B,$$

which is a superposition of different pointer settings, as well as a linear superposition of object states.

The next step is to extract some information about the object system A from the pointer system B. To be useful, the measurement of a particular value g_k for the pointer must tell you something about the object system A: to g_k must correspond a value for some observable F_A that addresses only properties of the object A.

Our clever experimentalist friends (Stern and Gerlach, for example) have set up their equipment so that each pointer reading g_k corresponds to f_k, one of the possible values of F_A. Assuming perfect correlation, the counter g_k corresponds to a particular eigenstate $|\,k\,\rangle_A$ of F_A with value f_k.

Expand the object states in terms of F_A eigenstates (assuming no degeneracies),

$$|\,a\,\rangle_A = \sum_k \sigma_{ak} |\,k\,\rangle_A,$$

so that

$$|\,\Psi\,\rangle_{AB} = \sum_{a,ik} \sigma_{ak}\omega_{a\,i} |\,k\,\rangle_A \otimes |\,i\,\rangle_B = \sum_{ik} \chi_{ik} |\,k\,\rangle_A \otimes |\,i\,\rangle_B.$$

The perfect correlation between g_k and f_k means that $\chi_{ik} = \chi_k \delta_{ik}$, yieldin the resulting ket after measurement of the form,

$$|\,\Psi\,\rangle_{AB} = \sum_k \chi_k |\,k\,\rangle_A \otimes |\,k\,\rangle_B,$$

It describes a state which is a mixture for each separate system (A or B). $p_k = |\chi_k|^2$ is the probability of finding the system A in the pure state $|\,k\,\rangle_A$ with eigenvalue f_k, or of finding system B in the pure state $|\,k\,\rangle_B$ with pointer reading g_k. The two mixtures are correlated by the measuring device as $g_k \to f_k$.

The Stern-Gerlach Experiment

A beam of (silver in the original experiment) atoms impinges on a region with a non-uniform magnetic field.

The object is a beam silver atoms. The apparatus is a magnet that produces a non-uniform magnetic field perpendicular to the incoming beam. The object-apparatus interaction generates from

$$H_{AB} = -\vec{\mu} \cdot \vec{B}(z),$$

where $\vec{\mu}$ is the atom's (object) magnetic moment. This generates a force

$$F_z = -\mu_z \frac{\partial B_z}{\partial z}.$$

Its effect is to deflect the trajectory of the atom according to the value of the z-component of its magnetic moment.

The measurement is the deflection of the beam in terms of a screen placed to the right. Alternatively we can block one beam and obtain only one "purified" beam. Measurement produces a pure state.

Walter Gerlach and Otto Stern find in 1922 that the beam of silver atoms splits into two beams after going through the inhomogeneous magnetic field.

Bauer and London consider a toy Stern-Gerlach experiment where the magnetic moment is in the $L = 1$ state so that the one beam is split into three. The object state has three state and the apparatus has three settings.

Before interaction between the beam and the magnetic field (called measurement by S-G), the density matrices are pure states

$$\rho_A = \begin{pmatrix} \psi_{-1}\psi_{-1}^* & \psi_{-1}\psi_0^* & \psi_{-1}\psi_1^* \\ \psi_0\psi_{-1}^* & \psi_0\psi_0^* & \psi_0\psi_1^* \\ \psi_1\psi_{-1}^* & \psi_1\psi_0^* & \psi_1\psi_1^* \end{pmatrix}, \quad \rho_B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

After "measurement", they become mixtures

$$\rho_A = \begin{pmatrix} |\psi_{-1}|^2 & 0 & 0 \\ 0 & |\psi_0|^2 & 0 \\ 0 & 0 & |\psi_1|^2 \end{pmatrix}, \quad \rho_B = \begin{pmatrix} |\psi_{-1}|^2 & 0 & 0 \\ 0 & |\psi_0|^2 & 0 \\ 0 & 0 & |\psi_1|^2 \end{pmatrix}$$

Note that they are the same since the measuring apparatus has been set up to be maximally correlated with the states of the object.

Von Neumann

In his analysis of measurement of quantum systems, Von Neumann considers three systems:

- A: The Observed System

- B: The Measuring Device

- C: The Observer

Our previous analysis concerned itself with the object-apparatus combination. The final step is the recording of the measurement by an "observer" who enters the process only at this time. It/he/she can be a human, a cat (not Schrödinger's!), a robot, or any other kind of recording device. Detailed knowledge of the observer (like age) is not necessary.

We should have started with the state living in three Hilbert spaces, producing through entanglement the linear superposition,

$$|\,\Psi\,\rangle_{ABC} = \sum_k \psi_k |\,k\,\rangle_A \otimes |\,0\,\rangle_B \otimes |\,0\,\rangle_C \;\;\longrightarrow\;\; |\,\Psi\,\rangle_{ABC} = \sum_k \chi_k |\,k\,\rangle_A \otimes |\,k\,\rangle_B \otimes |\,k\,\rangle_C,$$

where $|\,0\,\rangle_B$ is the ground state of the measuring device, $|\,0\,\rangle_C$ and $|\,k\,\rangle_C$ are the observer's ground and general states of the observer.

The object-apparatus system is represented by a mixture. The result of the observation is to transit from a mixed state to a pure state, suggesting that we think of it as a filter. The whole process correlates the outcome on a measuring device to an initial property of the object.

Make a slit on the recording screen at the end of the Stern-Gerlach apparatus, thereby allowing only atoms with a certain value of their magnetic moment through. But we do not know which individual atom is in the transmitted beam: "the filter produces pure cases, but in an absolutely **anonymous** form". Quantum Mechanics gives a definite answer on the species, not on the individual. Bauer and London whimsically call Quantum Mechanics "a theory of species"!

The amazing thing is that the result of a quantum measurements does not really depend on the split-up into three systems. Yet it is legitimate to ask how the result depends on the way we have broken up the boundaries. Von Neumann gives several examples:

Von Neumann puts measurements in two categories

- Process 1: Discontinuous Change ("Collapse of the Wavefunction") which is

I	System	System+Meter	Observer up to Retina
II	Meter	Light+Eye	Retina, Nerves+Brain
III	System +Meter+Light	Observer	Observer's Ego

not reversible, and amounts to projecting a pure state out of an initial state. This is akin to "before" and "after" commercials for hair coloring or weight loss, etc .

- Process 2: Continuous Change which proceeds by reversible unitary evolution.

As an example of the second version, he consider a physical system S with coordinate q and the Apparatus with coordinate r. Initially, before measurement, the Hamiltonian and wavefunction are given by

$$H = H^S + H^A, \quad \text{and} \quad \Psi^{S+A}(q,r) = \phi(q)\eta(r), \quad t < 0.$$

At $t = 0$ System and Apparatus interact through the Hamiltonian

$$H = H^S + H^A + H^{S+A}; \quad H^{S+A} = -i\hbar q \frac{d}{dr}.$$

It is readily solved, resulting in the wavefunction,

$$\Psi^{S+A}(q,r,t) = \phi(q)\eta(r - qt), \quad 0 < t < T.$$

The interaction is now switched off at $t = T$.

There are several ways to interpret this wavefunction. One is

$$\Psi^{S+A}(q,r,T) = \int dq' \phi(q')\psi(q',q,r),$$

where

$$\psi(q',q,r) = \delta(q' - q)\eta(r - q'T).$$

For each q' the apparatus is in a state displaced by $q'T$ and the total wavefunction is the superposition with the observer states $\phi(q')$.

Alternatively, the same wavefunction can be expanded in terms of the apparatus coordinates r'

$$\Psi^{S+A}(q,r,T) = \int dr' \delta(r - r') \frac{1}{N(r')} \xi(q,r').$$

The normalized

$$\xi(q, r') = N(r')\phi(q)\eta(r' - qT),$$

are the relative system wavefunctions for the apparatus states $\delta(r-r')$ of definite value $r = r'$. Furthermore if $\eta(r)$ is peaked, the $\xi(q, r')$ are nearly eigenstates for $q \approx r'/T$.

Everett puts it succinctly: "As a result of the interaction the state of the measuring apparatus is no longer capable of independent definition. It can be defined only relative to the state of the object system".

Both are correlated by the interaction. This analysis would imply indefinite behavior; yet the recording of a measurement always appears in a definite way!

Everett

Hugh Everett III proposes his *"Relative State" Formulation of Quantum Mechanics* (Rev. Mod. Phys. **29**, 454 (1957)). He is motivated as much by Von Neumann's analysis of measurement as by his desire to achieve consistency with General Relativity.

General Relativity allows space-time geometries for closed universes. The three components associated with measurements, object, apparatus and observer are all part of the same system and must be considered together. There is no such thing as an external observer. The observer is part of the whole.

He rejects the notion of an external observer who views measurement as a series of irreversible projection operators on the initial wavefunction. Quantum Mechanics proceeds through reversible unitary evolution, as in Von Neumann's measurement example.

This means that the different parts of the measurement process lose their individuality. In his language, when looking at an interacting state only relative states have meaning.

Everett posits that the observer states have memories of previous measurements. He writes the observer states in the form

$$|\, \psi_{[\alpha,\beta,\ldots,\gamma]} \,\rangle^{\mathrm{O}},$$

where $[\alpha, \beta, \ldots, \gamma]]$ represent a string of measured values. In Quantum Mechanics they are eigenvalues of hermitian operators, the only allowed observables.

Start with the state ket $|\, \alpha_i \,\rangle^{\mathrm{S}}$, an eigenstate of the system's hermitian operator A with eigenvalue α_i. The act of observation changes the state ket

$$|\,\Psi\,\rangle^{\mathrm{S+O}} = |\,\alpha_i\,\rangle^{\mathrm{S}} \otimes |\,\psi_{[\ldots]}\,\rangle^{\mathrm{O}} \quad \longrightarrow \quad |\,\Psi\,\rangle^{\mathrm{S+O}'} = |\,\alpha_i\,\rangle^{\mathrm{S}} \otimes |\,\psi_{[\ldots,\alpha_i]}\,\rangle^{\mathrm{O}}.$$

The system remains unchanged if it is an eigenstate of A. The process is repeatable as a second measurement of the same observable yields

$$|\,\Psi\,\rangle^{\mathrm{S+O}''} = |\,\alpha_i\,\rangle^{\mathrm{S}} \otimes |\,\psi_{[\ldots,\alpha_i,\alpha_i]}\,\rangle^{\mathrm{O}}.$$

When the system is not in an eigenstate of A, we expand its state in A eigenkets $|\,\psi\,\rangle = \sum_i a_i |\,\alpha_i\,\rangle$, with $a_i = \langle\,\alpha_i\,|\,\psi\rangle$. Measurement generalizes by superposition,

$$|\,\Psi\,\rangle^{\mathrm{S+O}} = \sum_i a_i |\,\alpha_i\,\rangle^{\mathrm{S}} \otimes |\,\psi_{[\ldots]}\,\rangle^{\mathrm{O}} \quad \longrightarrow \quad \sum_i a_i |\,\alpha_i\,\rangle^{\mathrm{S}} \otimes |\,\psi_{[\ldots,\alpha_i]}\,\rangle^{\mathrm{O}}.$$

It is a linear combination of states each of which has a different observer state.

If the object is made up of several systems,

$$|\,\chi_1^{\mathrm{S_1}}\,\chi_2^{\mathrm{S_2}}\,\cdots,\chi_n^{\mathrm{S_n}}\,\rangle \equiv |\,\chi_1\,\rangle^{\mathrm{S_1}} \otimes |\,\chi_2\,\rangle^{\mathrm{S_2}} \otimes \cdots \otimes |\,\chi_n\,\rangle^{\mathrm{S_n}},$$

a measurement of A in the first system yields

$$|\,\chi_1^{\mathrm{S_1}}\,\chi_2^{\mathrm{S_2}}\,\cdots,\chi_n^{\mathrm{S_n}}\,\rangle |\,\psi_{[\ldots]}\,\rangle^{\mathrm{O}} \quad \longrightarrow \quad \sum_i a_i |\,\alpha_i\,\rangle^{\mathrm{S_1}} |\,\chi_2^{\mathrm{S_2}}\,\cdots,\chi_n^{\mathrm{S_n}}\,\rangle |\,\psi_{[\ldots,\alpha_i]}\,\rangle^{\mathrm{O}}$$

with

$$|\,\chi_1\,\rangle^{\mathrm{S_1}} = \sum_i a_i |\,\alpha_i\,\rangle^{S_1}.$$

A further measurement of another observable B on $\mathrm{S_2}$ yields,

$$\sum_i a_i |\,\alpha_1\,\rangle^{\mathrm{S_1}} |\,\chi_1^{\mathrm{S_1}}\,\chi_2^{\mathrm{S_2}}\,\cdots\chi_n^{\mathrm{S_n}}\,\rangle |\,\psi_{[\ldots,\alpha_i]}\,\rangle^{\mathrm{O}} \quad \longrightarrow \quad \sum_{i,j} a_i b_j |\,\alpha_i\,\rangle^{\mathrm{S_1}} |\,\beta_j\,\rangle^{\mathrm{S_2}} |\,\chi_3^{\mathrm{S_3}}\cdots\chi_n^{\mathrm{S_n}}\,\rangle |\,\psi_{[\ldots,\alpha_i,\beta_j]}\,\rangle^{\mathrm{O}}$$

with

$$|\,\chi_2\,\rangle^{\mathrm{S_2}} = \sum_j b_j |\,\beta_j\,\rangle^{\mathrm{S_2}}, \cdots,$$

expanded in the B eigenkets $|\,\beta_j\,\rangle^{S_2}$. The result is a double superposition of states, with a different observer state for each.

Now for something different: an observer measures the same quantity, e.g. A eigenvalues, in many identical states S_1, S_2, $\cdots$, S_n. After r measurements, the resulting ket is

$$|\,\Psi\,\rangle_r = \sum_{i,j,\ldots,k} a_i a_j \cdots a_k |\,\alpha_i\,\rangle^{\mathrm{S}_1} |\,\alpha_j\,\rangle^{\mathrm{S}_2} \cdots |\,\alpha_j\,\rangle^{\mathrm{S}_\mathrm{r}} |\,\psi_{[\cdots,\alpha_i^1,\alpha_j^2,\ldots,\alpha_k^r]}\,\rangle^{\mathrm{O}}.$$

The object states are left in their original configurations while the observer has observed a sequence of definite results. This sequence is not necessarily random because if an earlier system $\mathrm{S_l}$ is measured to give α_s^l, a second measurement of the same system will necessarily give the same result, α_s^l. Hence these numbers are not independent but correlated.

It seems to the observer that the $\mathrm{S_l}$ system has become stuck in the same configuration. Roughly speaking then, the state of that system has been projected in a substate where in the sense of eigenvalues $A = \alpha_s^l$.

The one observer is represented by different states depending on what it has measured (its memory). The observer state (not the observer!) branches out with each observation into a different state. The observer is not aware of this branching out, and the trajectory of the memory configuration is a branching tree, with all outcomes existing simultaneously. Each state in the linear combination is a history, and the full state ket is a linear combination of all possible histories.

Everett's interpretation was called the multi-world formulation of quantum mechanics by Bryce DeWitt. Do not be misled by the name: these different worlds do not communicate with one another. For the moment it is a more pleasing description of the measurement process because it evolves through unitary evolution.

The next step is to assign a probability or weight to each history (state) in the linear combination. The unique choice assigns to each history

$$|\,\alpha_i\,\rangle^{\mathrm{S}_1} |\,\alpha_j\,\rangle^{\mathrm{S}_2} \cdots |\,\alpha_j\,\rangle^{\mathrm{S}_\mathrm{r}} |\,\psi_{[\cdots,\alpha_i^1,\alpha_j^2,\ldots,\alpha_k^r]}\,\rangle^{\mathrm{O}}$$

the weight

$$M_{ij\ldots k} = (a_i a_j \cdots a_k)^* (a_i a_j \cdots a_k),$$

the product of $M_i M_j \cdots M_k$, of the weights for the individual components of the memory sequence.

Suppose our observer has performed a very large number of measurements. Each memory sequence will look like a randomly generated sequence with independent probabilities $a_i^* a_i$.

Consider a memory sequence $[\alpha_1, \cdots, \alpha_j, \cdots, \alpha_k]$, with each value generated independently with probability $a_j^* a_j$. If the number of measurements is large enough, the correlation will disappear so that we are justified as thinking of the outcome as if the system had been projected into these states. Everett's concludes:

"Except for a set of memory sequences of measure nearly zero, the averages of any functions over a memory sequence can be calculated approximately by the use of independent probabilities given by Process 1 ("collapse of the wavefunction") for each initial observation, on a system, and by the use of the usual transition probabilities for succeeding observations upon the same system. In the limit, as the number of all types of observations goes to infinity the calculation is exact, and the exceptional set has measure zero."

This analysis is generalized to different measurements. When several observers have separately observed the same quantities and then communicated the results to one another, they are in agreement.

In the famous EPR paradox, two observers measure properties of a correlated but non-interacting system, such as two independent spins (in David Bohm's formulation). The first observes the first spin, and the second observes the second spin. Let observer 1 make a measurement on the correlated state, followed by observer 2 "measuring" the second spin. In Everett's formulation, if the first observer repeats its measurement it finds the same result as before.

There is no EPR paradox: it's just Quantum Mechanics!

It allows us to find an alternate expressions for the density matrices. Since

$$\mathrm{Tr}_B \mathcal{O} = \sum_j \langle\, j^B \,|\mathcal{O}|\, j^B \,\rangle,$$

we find

$$\rho^A = \mathrm{Tr}_B \big[|\, \Psi^{AB} \,\rangle\langle\, \Psi^{AB} \,| \big], \qquad \rho^B = \mathrm{Tr}_A \big[|\, \Psi^{AB} \,\rangle\langle\, \Psi^{AB} \,| \big],$$

using the orthonormality of the bases. Note that the same non-zero probabilities p_i appear in both expressions although the A and B systems will differ in their number of zero eigenvalues.

The"information" contained in a quantum state with density matrix ρ is given by the von Neumann entropy,

$$S(\rho) = -\mathrm{Tr}[\rho \log \rho].$$

- The entropy of a pure state for which ρ has one non-zero eigenvalue vanishes.

- The entropy of a compound state ρ^{AB} satisfies the subadditivity constraint,

$$S(\rho^{AB}) \leq S(\rho^A) + S(\rho^B),$$

which states that the information in the compound state is less than the total input information: information has been lost in forming the compound state.

Applying these to the Schmidt decomposition, we find,

$$S(\rho^{AB}) = 0 \quad \longrightarrow \quad S(\rho^A) = S(\rho^B) \geq 0.$$

An important application is the association of a pure state to an impure state in a process called *purification*. Given a mixture density matrix ρ^A, with ket $|\, \psi^A \,\rangle$, we adjoin another Hilbert space $\mathcal{H}_B$ and form the pure state,

$$|\, \psi^{AB} \,\rangle = |\, \psi^A \,\rangle \otimes |\, \phi^B \,\rangle, \qquad \rho^{AB} = \rho^A \otimes |\, \phi^B \,\rangle\langle\, \phi^B \,|,$$

where $|\, \phi^B \,\rangle$ is any normalized state in $\mathcal{H}_B$.

The original density matrix is the partial trace over B of the AB density matrix

$$\rho^A = \mathrm{Tr}_B \big[\rho^{AB}\big] = \mathrm{Tr}_B \big[|\, \psi^{AB} \,\rangle\langle\, \psi^{AB} \,| \big],$$

It looks like a cheap trick (it is!), but it allows for different ways of expressing the physics of the A system.

act of observation is macroscopic

it appears in QM that the result of observations is intimately tied up with the consciousness of he who makes it and that qm thus leads us to a complete solipsism (knowledge outside of one's mind is unsure) sol-ipsis: only oneself.

filter does not take an individual object into a pure state, but it does take an individual object into a mixture.

0.1 Schumacher

Notes from Benjamin Schumacher, *Quantum Coding*, Phys. Rev. A **51** 2738 (1995).

Three different meanings of entropy.

- In Information Theory, entropy is the Shannon entropy $H(A)$, where A is a message source that produces message a with probability $p(a)$, represented by a sequence of binary bits that are as short as possible. Shannon entropy $H(A)$ is the mean number of bits necessary to code the output of A and still reconstruct the message:

$$\bar{L} \geq H(A): \qquad \text{Noiseless Coding Theorem.}$$

- In Statistical Mechanics, entropy is a measure of disorder of a physical system. To link with information theory, the entropy of a macrostate is the number of bits required to specify the microstate of the system.

- In Quantum Systems, entropy is $S(\rho)$ as defined by Von Neumann where ρ is the density matrix. It is the same as Shannon's only if $p(a)$ are interpreted as eigenvalues of hermitian operator A.

They are in general different. Let A be a quantum signal source with messages a encoded into signal states $|\, a_M \,\rangle$ of a quantum system M: $A \to a \to M$. The ensemble of signals is represented by the density operator,

$$\rho = \sum_a p(a) |\, a_M \,\rangle\langle\, a_M \,|.$$

If the signal states are orthogonal to one another, it is possible to distinguish them from one another, and the Von Neumann and Shannon entropies are the same.

In general, the signal states may not be orthogonal, so that

$$S(\rho) < H(A).$$

In order to do so, consider " accessible" information, the maximum information that can be recovered by measuring something on M.

Mutual information for two random variables X and Y,

$$H(X:Y) = H(X) + H(Y) - H(X,Y), \quad H(X,Y),$$

is the amount of information about X acquired by determining the value of Y.

Accessible information is bounded by $S(\rho)$: Kholev's theorem

Quantum Coding Theorem: Von Neumann entropy of an ensemble is the mean number of qubits necessary to encode the states in the ensemble of an ideal coding scheme

Quantum information cannot be cloned, so in order to transmit is the best we can do is to transpose it by adding to the original Hilbert space $\mathcal{H}_M$ a

new Hilbert space $\mathcal{H}_X$ of dimensions at least as large as the original one. The operation

$$M \quad \rightarrow \quad X \quad \rightarrow \quad M'$$

where X is the quantum channel, and M' is the decoded quantum system, has to be performed by unitary transformations. In terms of quantum states,

$$|\, a_M, 0_X \,\rangle \quad \rightarrow \quad |\, 0_M, a_X \,\rangle$$

performed by a unitary transformation $\mathcal{U}$ so as to preserve the inner products. The inverse transformation gets us back to M. This is a one-to-one transmission of a quantum state.

Now suppose that we do not send all of the signal in X to M'. How much of this approximate transposition can we get away with and still make a very small number of errors?

Set $X = C + E$, where only C is transmitted to the receiver. Then the sequence of operations is

$$M \quad \rightarrow \quad C + E \quad \rightarrow \quad C \quad \rightarrow \quad C + E' \quad \rightarrow \quad M'$$

where we have added/subtracted Hilbert spaces $\mathcal{H}_{E,E'}$.

Start with a state $|\, a_M \,\rangle$ in M, with density matrix $\pi_a = |\, a_M \,\rangle\langle\, a_M \,|$, and end up in M' with a state represented by the transmitted density matrix w_a. For this signal, the fidelity will be $\mathrm{Tr}(\pi_a w_a)$. For an initial set of states with probability $p(a)$, a natural definition of the *fidelity* F is

$$F = \sum_a p(a)\mathrm{Tr}(\pi_a w_a),$$

which varies between zero and one. Then

$$F = \sum_a p(a)\mathrm{Tr}(\Pi_a W_a),$$

where Π_a and W_a are the density matrices in $C + E$ and $C + E'$ respectively.

0.2 Schumacher-Nielsen

A general analysis of split Hilbert spaces in terms of kets and entropy is presented in the paper by Schumacher and Nielsen[**?**].

Consider an impure quantum state described by the density operator ρ^Q acting in a Hilbert space $\mathcal{H}_Q$. We want to study its evolution,

$$\rho^Q \quad \longrightarrow \quad \rho^{Q'} = \mathcal{E}^Q(\rho^Q),$$

where $\mathcal{E}^Q$ is a trace-preserving linear mapping of positive probabilities into positive probabilities. The usual representation is,

$$\rho^{Q'} = \mathcal{U}^Q \rho^Q \mathcal{U}^{Q\dagger},$$

where $\mathcal{U}^Q$ is a unitary matrix.

Adjoin to $\mathcal{H}_Q$ a reference Hilbert space $\mathcal{H}_R$, to purify the original state in the compound space to $|\,\psi^{RQ}\,\rangle$ with density matrix,

$$\rho^{RQ} = |\,\psi^{RQ}\,\rangle\langle\,\psi^{RQ}\,| = \rho^Q \otimes \rho^R, \qquad \rho^R = |\,\phi^R\,\rangle\langle\,\phi^R\,|$$

where $|\,\phi^R\,\rangle$ is any normalized state in $\mathcal{H}_R$. This allows us to express the evolution of the physical system in a new form,

$$\rho^{Q'} = \mathrm{Tr}_E\big[\mathcal{U}^{RQ}(\rho^Q \otimes |\,0^R\,\rangle\langle\,0^R\,|)\mathcal{U}^{RQ\dagger}\big],$$

where the unitary matrix $\mathcal{U}^{RQ}$ "entangles" the Q and R systems.

A third representation of the evolution operator is obtained by writing the Q-system density matrix in its canonical form $\rho^Q = \sum_k p_k |\,k^Q\,\rangle\langle\,k^Q\,|$. Expressing the partial trace over the basis states $|\,j^R\,\rangle$,

$$\rho^{Q'} = \sum_j \sum_k p_k \big[\langle\, j^R\,|\mathcal{U}^{RQ}|\,\phi^R\,\rangle|\,k^Q\,\rangle\big]\big[\langle\, k^Q\,|\langle\,\phi^R\,|\mathcal{U}^{RQ\dagger}|\,j^R\,\rangle\big].$$

Defining the operator

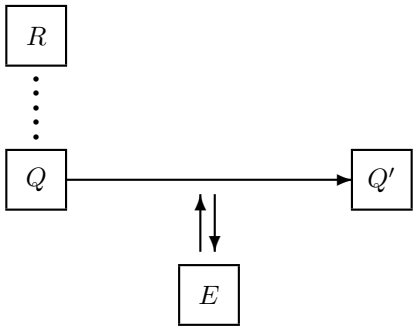
$$A_j^Q = \langle\, j^R\,|\mathcal{U}^{RQ}|\,\phi^R\,\rangle, \qquad \sum_j A_j^{Q\dagger} A_j^Q = 1^Q,$$

yields the operator sum representation,

$$\rho^{A'} = \sum_j A_j^Q \rho^Q A_j^{Q\dagger}.$$

To summarize, the reference system is introduced to purify the initial state, and allow for more representations of the unitary evolution.

The same formalism can be generalized to describe the entanglement of the physical system with its environment E. In that case we are dealing with three Hilbert spaces $\mathcal{H}_Q$, $\mathcal{H}_R$ and $\mathcal{H}_E$, and a total purification $|\,\psi^{RQE}\,\rangle$.



We start with the pure state $|\,\psi^{RQE}\,\rangle$,

$$|\,\psi^{RQE}\,\rangle = |\,\psi^{Q}\,\rangle \otimes |\,0^{R}\,\rangle \otimes |\,0^{E}\,\rangle,$$

with the initial reference and environment states arbitrarily set. After evolution, the full system is given by another pure state

$$|\,\psi^{RQ'E'}\,\rangle = (\mathbf{1}^{R} \otimes \mathcal{U}^{QE})|\,\psi^{RQE}\,\rangle.$$

We can define several properties that are intrinsic to the Q system:

Entanglement Fidelity F_e is the value of the entangled density operator in the initial pure state,

$$F_e = \langle\,\psi^{RQ}\,|\rho^{RQ'}|\,\psi^{RQ}\,\rangle,$$

Using the Schmidt representation,

$$|\,\psi^{RQ}\,\rangle = \sum_k \sqrt{p_k}|\,k^{R}\,\rangle \otimes |\,\phi_k^{Q}\,\rangle$$

we find that for any operator X^Q,

$$\langle\,\psi^{RQ}\,|(1 \otimes X^{Q})|\,\psi^{RQ}\,\rangle = \sum_k p_k \langle\,\phi_k^{Q}\,|X^{Q}|\,\phi_k^{Q}\,\rangle = \mathrm{Tr}[\rho^{Q} X^{Q}]$$

$$F_e = \sum_j \mathrm{Tr}[\rho^{Q} A_j^{Q}]\mathrm{Tr}[\rho^{Q} A_j^{Q\dagger}]$$

showing that Entanglement Fidelity is intrinsic to the Q system.

Entropy Exchange S_e is a measure of the information exchanged between the system Q and the rest of the world during the evolution $\mathcal{E}^Q$. It is the difference between the final and initial entropies,

$$S_e = S(\rho^{RQ'}) - S(\rho^{RQ}) = S(\rho^{RQ'}) = -\mathrm{Tr}[\rho^{RQ'} \log \rho^{RQ'}],$$

since ρ^{RQ} describes a pure state. Since $RQ'E'$ is a pure state, we also have

$$S_e = S(\rho^{E'}),$$

the entropy of the environment.

The entropy exchange is independent of purification because while different purifications lead to $\rho_1^{RQ'}$ and $\rho_2^{RQ'}$, with the same eigenvalues, and thus the same von Neumann entropies,

$$S(\rho_1^{RQ'}) = S(\rho_2^{RQ'}).$$

Starting from

$$\rho^{RQ'} = \sum_j (1^R \otimes A_j^Q)\rho^{RQ}(1^R \otimes A_j^Q)^\dagger,$$

a little bit of work shows that, S_e is an intrinsic property of the Q system,

$$S_e = -\mathrm{Tr}[\mathbf{W} \log \mathbf{W}],$$

where

$$\mathbf{W} = \{w_{ij} = \mathrm{Tr}[A_i^Q \rho^Q A_j^{Q\dagger}]\}.$$

Coherent Quantum Information I_e *"serves as a natural measure of the degree to which quantum coherence is retained by the dynamical process* $\mathcal{E}^Q$,

$$I_e \equiv S(\rho^{Q'}) - S(\rho^{RQ'}).$$

Its definition means that it determines the degree of coherence that remains after the evolution $\mathcal{E}^Q$. In addition

$$I_e = S(\rho^{Q'}) - S_e = S(\rho^{Q'}) - S(\rho^{E'}),$$

and the last equality shows I_e as the difference of information in the Q system and in the environment E system.

Since $RQ'E'$ is a pure state,

$$I_e = S(\rho^{RE'}) - S(\rho^{E'}),$$

and the subadditivity of the entropy yields,

$$S(\rho^{RE'}) \leq S(\rho^R) + S(\rho^{E'}),$$

but RQ is also a pure state, that is

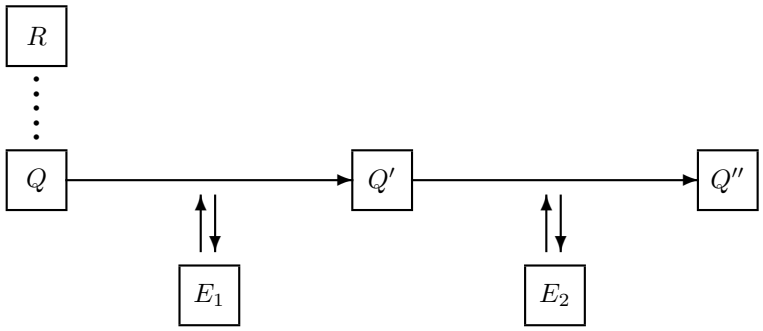
$$I_e \leq S(\rho^R) = S(\rho^{R'}),$$

allowing us to conclude with the inequality,

$$S(\rho^Q) \geq S(\rho^{Q'}) - S_e = I_e.$$

The coherent information is no greater than the initial information

Consider the two-stage evolution:



It starts with the pure state $|\,\psi^{RQE_1E_2}\,\rangle$,

$$|\,\psi^{RQE_1E_2}\,\rangle = |\,\psi^{Q}\,\rangle \otimes |\,0^{R}\,\rangle \otimes |\,0_1^{E}\,\rangle \otimes |\,0_2^{E}\,\rangle,$$

with the initial reference and environment states chosen arbitrarily. Evolution proceeds in two stages. The first stage yields

$$|\,\psi^{RQ'E_1'E_2}\,\rangle = (\mathbf{1}^{R} \otimes \mathcal{U}^{QE_1} \otimes \mathbf{1}^{E_2})|\,\psi^{RQE_1E_2}\,\rangle,$$

and the second stage,

$$|\,\psi^{RQ''E_1'E_2''}\,\rangle = (\mathbf{1}^{R} \otimes \mathbf{1}^{E_1} \otimes \mathcal{U}^{QE_2})|\,\psi^{RQ'E_1'E_2}\,\rangle.$$

Schumacher and Nielsen apply the strong subadditivity of entropy,

$$S(\rho^{ABC}) + S(\rho^{B}) \leq S(\rho^{AB}) + S(\rho^{B})$$

Analysis (to be filled) leads to the inequalities

$$\begin{aligned} S(\rho^Q) &\geq S(\rho^{Q'}) - S_{e1} \geq S(\rho^{Q''}) - S_{e12} \\ &\geq I_{e1} \geq I_{e12}. \end{aligned} \tag{1}$$

Let us suppose that the second stage is an error-correcting code. Then it is reasonable to assume that the entanglement fidelity F_{e12}, is equal to one: the initial entanglement of the Q system with the reference system R is completely restored. This means that the initial and final states have the same density matrices,

$$\rho^{Q''} = \rho^{Q}.$$

In classical probability theory, the Fano inequality relates the probability of errors to the noise in the transmission of information in a channel. Schumacher derives the quantum equivalent as follows.

Let the system RQ evolves into RQ', and take both Hilbert spaces $\mathcal{H}_Q$ and $\mathcal{H}_R$ to have dimension d. There are d^2 possible states available for measurement. One state is the original $|\,\psi^{QR}\,\rangle$, with probability F_e. The Shannon entropy assumes its maximal value when all the remaining $d^2 - 1$ states have equal probability, $(1 - F_e)/(d^2 - 1)$. A simple computation yields,

$$\max H = h(F_e) + (1 - F_e)\log(d^2 - 1), \qquad h(x) = -x\log x - (1 - x)\log(1 - x).$$

but the von Neumann entropy is a lower bound to the Shannon entropy, so that we obtain the quantum Fano inequality,

$$h(F_e) + (1 - F_e)\log(d^2 - 1) \geq S_e.$$

Thus if $F_e = 1$, it follows that $S_e = 0$.

The entropy exchange of the whole process S_{e12} must vanish. Putting it all together, the inequalities (1) imply that

$$S(\rho^{Q}) \geq S(\rho^{Q'}) - S_{e1} \geq S(\rho^{Q''}) = S(\rho^{Q}),$$

that is

$$S(\rho^{Q}) = I_{e1},$$

the coherent information of the channel equals the entropy of the input state. Actually this equation is a both necessary and sufficient condition for the existence of a perfect error-correcting code.

Perfect quantum error correction is possible only if the environment obtains no information about the state of the system Q.

RSA Encryption

Encoding and decoding schemes of secret messages had traditionally been symmetric between senders and receivers. In 1970, James Ellis, at the Government Communications Headquarters (GCHQ), UK's equivalent of US's NSA, suggested that non-secret encryption and decryption could be asymmetric.

The next step belonged to Clifford Cocks who invented in 1973 the concept of a trap door, using prime number factorization. However his invention was kept secret by GCHQ.

In 1977, unaware of Ellis and Cocks' previous work, Ronald Rivest, Adi Shamir, and Leonard Adleman re-invented the trap-door scheme.

Let G_p denote the positive integers up to $p-1$, where p is a prime. Fermat's little theorem states that if $a \in G_p$, then

$$a^{(p-1)} = 1, \pmod{p}.$$

To see this, let $a = 1 + b$. Then $(1 + b)^p = 1 + \cdots + b^p = (1 + b), \pmod{p}$, because the dots are terms proportional to p. It extends to two primes, p and q,

$$a^{(p-1)(q-1)} = 1 \pmod{pq}.$$

We now raise this equation to an integer power k and multiply it by a to get

$$a^{1+k(p-1)(q-1)} = a \pmod{pq}.$$

Let c be an integer in $G_{(p-1)(q-1)}$ with no factor in common with $(p-1)(q-1)$. Its inverse d must also be in $G_{(p-1)(q-1)}$. Setting $cd = 1 + k(p-1)(q-1)$,

$$a^{cd} = 1 \pmod{pq}.$$

It follows that if $b \equiv a^c \pmod{pq}$, then $b^d \equiv a \pmod{pq}$. This is the basis of the RSA scheme.

A later version of the RSA scheme uses Euler's totient function defined as

$$\varphi(n) = \prod_{n|p}(1 - \frac{1}{p}),$$

with the product taken over prime numbers which divide n. It counts the positive integers up to a given integer n that are relatively prime to n. Some of its salient properties for prime p, q:

$$\varphi(p) = (p-1); \quad \varphi(p^k) = p^{k-1}(p-1); \quad \varphi(p\,q) = (p-1)(q-1).$$

Euler's theorem states that if a and n are relative primes then

$$a^{\varphi(n)} = 1 \pmod{n}.$$

For n prime, it reduces to Fermat's little theorem.

Encryption Procedure

Bob picks two primes, p and q, and an integer c which has no common factors with $(p-1)(q-1)$. He computes its inverse d, with $cd = 1, (\text{mod } n = pq)$.

Bob sends $n = pq$ and c to Alice, but **not** the individual primes. n and c are the public key of the RSA scheme.

Alice wants to send a message m. She forms the integer $b = m^c, \pmod{n}$, and sends it to Bob.

After receiving b, Bob who knows d, easily finds m by taking the dth power of b since

$$b^d = m^{cd} = m \pmod{n}.$$

The only pieces of data made public were the N and c by Bob, and b by Alice.

All three could have been intercepted by Eve(sdroppersky). However, knowing only n and c, she does not know how to get

$$d = \frac{1 + k\varphi(n)}{c},$$

because it requires knowing $\varphi(n)$. For very large n this could take as much time as the age of the universe!

0.3 Threshold Schemes

If one does not want to trust information with one person, one trick is to share it in the form of partial information among a number of persons, with the ability to reconstruct the information sent to a subset of recipients.

They are called $((k,n))$ threshold schemes, with $k \leq n$. Information is split into n equal shares with incomplete information. It takes k shares to be able to reconstruct the information.

Cleve, Gottesman and Lo[**?**] provided in 1999 a quantum example with one qutrit, among 3^3 states $|\, x_1x_2x_3 \,\rangle$ where the x_i belong to $GF(3)$, $x_i = 0, 1, 2$ with (mod 3) composition.

The three base kets for the special qutrit are,

$$\begin{aligned} |\, \tilde{0} \,\rangle &= \frac{1}{\sqrt{3}}(|\, 000 \,\rangle + |\, 111 \,\rangle + |\, 222 \,\rangle), \\ |\, \tilde{1} \,\rangle &= \frac{1}{\sqrt{3}}(|\, 012 \,\rangle + |\, 120 \,\rangle + |\, 201 \,\rangle), \\ |\, \tilde{2} \,\rangle &= \frac{1}{\sqrt{3}}(|\, 021 \,\rangle + |\, 102 \,\rangle + |\, 210 \,\rangle). \end{aligned}$$

Their special property is the unitary operator $\mathcal{U}_{12}$ acting on the first two entries of the kets, such that

$$\mathcal{U}_{12}|\, \tilde{i} \,\rangle = |\, i \,\rangle \otimes \frac{1}{\sqrt{3}}(|\, 00 \,\rangle + |\, 21 \,\rangle + |\, 12 \,\rangle).$$

The action of $\mathcal{U}_{12}$ is in two steps; the first adds the first entry to the second entry of the ket, and the second step adds the second entry to the first, all (mod 3),

$$\mathcal{U}_{12}: \quad |\, i,j \,\rangle \;\rightarrow\; |\, i, i+j \,\rangle \;\rightarrow\; |\, 2i+j, i+j \,\rangle.$$

For example $|\, 10 \,\rangle \rightarrow |\, 11 \,\rangle \rightarrow |\, 21 \,\rangle$. The action of $\mathcal{U}_{12}$ on an arbitrary qutrit state,

$$|\, \tilde{\psi} \,\rangle = \alpha|\, \tilde{0} \,\rangle + \beta|\, \tilde{1} \,\rangle + \gamma|\, \tilde{2} \,\rangle$$

is given by

$$|\, \tilde{\psi} \,\rangle \;\rightarrow\; |\, \psi' \,\rangle = \mathcal{U}_{12}|\, \tilde{\psi} \,\rangle = (\alpha|\, 0 \,\rangle + \beta|\, 1 \,\rangle + \gamma|\, 2 \,\rangle) \otimes (|\, 00 \,\rangle + |\, 21 \,\rangle + |\, 12 \,\rangle),$$

where the last two entries of the ket always appear in the same linear combination.

One can define unitary operators $\mathcal{U}_{13}$ and $\mathcal{U}_{23}$, with the same results. So if we have information on any two out of the three qutrits, we can use them to reconstruct the original quantum state.

Almeheiri, Dong, and Harlow's convention[**?**] is slightly different,

$$\mathcal{U}_{12}|\,\tilde{i}\,\rangle = |\,i\,\rangle \otimes \frac{1}{\sqrt{3}}(|\,00\,\rangle + |\,11\,\rangle + |\,22\,\rangle) \quad \text{ADH}$$

$$|\,\psi\,\rangle \quad \rightarrow \quad (\alpha|\,0\,\rangle + \beta|\,1\,\rangle + \gamma|\,2\,\rangle) \otimes (|\,00\,\rangle + |\,11\,\rangle + |\,22\,\rangle) \quad \text{ADH}.$$

The quantum sharing procedure proceeds as follows: Encode an arbitrary state

$$|\,\psi\,\rangle = \alpha|\,0\,\rangle + \beta|\,1\,\rangle + \gamma|\,2\,\rangle \quad \rightarrow \quad |\,\tilde{\psi}\,\rangle = \alpha|\,\tilde{0}\,\rangle + \beta|\,\tilde{1}\,\rangle + \gamma|\,\tilde{2}\,\rangle.$$

As we have seen the original state can be read by applying any of the three the unitary transformations $\mathcal{U}_{ij}$.

However we do not trust all this information with one sender and we provide only partial information called shares to each sender.

Assume three senders, and provide each with a share. that contains information about one of the three qutrits.

Each sender does not have sufficient information to reconstruct the message, but two senders can reconstruct the original information, using the unitary operators $\mathcal{U}_{ab}$.

If one knows two out of three qutrits, one can use any of the three U_{12}, U_{23}, U_{13} to reconstruct the third

A share contains information about one qutrit.

1 Quantum Teleportation

Bennett *et al*[**?**] proposed a method to transport a quantum state from one place to another, using correlated EPR pairs. It requires three Hilbert space. One spin one-half particle lives in the first Hilbert space, with ket,

$$|\,\phi\,\rangle_1 = a|\uparrow\rangle_1 + b|\downarrow\rangle_1$$

The second and third Hilbert spaces sustain an entangled EPR pair of particles,

$$|\,\Psi^{\rm EPR}\,\rangle_{23} = \frac{1}{\sqrt{2}}\big[|\uparrow\rangle_2|\downarrow\rangle_3 - |\downarrow\rangle_2|\uparrow\rangle_3\big]$$

The state vector of the three particles is given by

$$|\,\Psi\,\rangle_{123} = |\,\phi\,\rangle_1 \otimes |\,\Psi^{\rm EPR}\,\rangle_{23}.$$

The sender (Alice) operates in the first two Hilbert spaces only. An EPR-inspired basis for her is

$$|\,\Psi^{\rm EPR}\,\rangle_{12} = \frac{1}{\sqrt{2}}\big(|\uparrow\rangle_1|\downarrow\rangle_2 \pm |\downarrow\rangle_2|\uparrow\rangle_1\big),$$

together with three remaining state vectors,

$$\begin{aligned} |\,\Phi^{(0)}\,\rangle_{12} &= \frac{1}{\sqrt{2}}\big(|\uparrow\rangle_1|\downarrow\rangle_2 + |\downarrow\rangle_2|\uparrow\rangle_1\big), \\ |\,\Phi^{(\pm)}\,\rangle_{12} &= \frac{1}{\sqrt{2}}\big(|\uparrow\rangle_1|\uparrow\rangle_2 \pm |\downarrow\rangle_1|\downarrow\rangle_2\big). \end{aligned}$$

Alice expresses $|\,\Psi\,\rangle_{123}$ in terms of these four orthogonal vectors,

$$\begin{aligned} |\,\Psi\,\rangle_{123} &= |\,\Psi^{\rm EPR}\,\rangle_{12} \otimes \big(-a|\uparrow\rangle_3 - b|\downarrow\rangle_3\big) + |\,\Phi^{(0)}\,\rangle_{12} \otimes \big(-a|\uparrow\rangle_3 + b|\downarrow\rangle_3\big) \\ &\quad + |\,\Phi^{(+)}\,\rangle_{12} \otimes \big(-b|\uparrow\rangle_3 + a|\downarrow\rangle_3\big) + |\,\Phi^{(-)}\,\rangle_{12} \otimes \big(b|\uparrow\rangle_3 + a|\downarrow\rangle_3\big), \\ &\equiv \sum_{i=1}^{4} |\,i\,\rangle_{12}|\,\phi^i\,\rangle_3. \end{aligned}$$

She can perform a von Neumann experiment, "collapsing" the state vector in four equally likely ways, so that Bob receives four possible states for his third particle.

Depending on her measurement, Alice sends Bob by snailmail a set of instructions which read

Depending on Alice's measurement, Bob's third particle has been projected in one of four quantum states

$$|\,\phi^1\,\rangle_3 = -|\,\phi\,\rangle_3, \qquad |\,\phi^2\,\rangle_3 =, \qquad |\,\phi^3\,\rangle_3 =, \qquad |\,\phi^4\,\rangle_3 =$$