Lectures on Quantum Information

Ru Shihao
Department of Applied Physics,
Xi'an JiaoTong University

2/28, 2018

Contents

Chapter 1

TWO-LEVEL SYSTEMS

1.1 Generalities

- Two-level Systems: Systems that are described by two states, i.e. their states belong to a Hilbert space of dimension 2, $\mathcal{H}_2$. These two states will be denotes by $|1\rangle$ and $|2\rangle$. Some times the two-level systems are called quantum bits (qubits);

- Importance: They are very important since in many problems only two states of a given system participate, so that one can describe the problem exactly with a two-level system description;

- Examples: There are many physical situations where the two-level description suffices:

  (a) Two-level Atom: An atom has infinite internal levels ($|n, l, m, s\rangle$, for the hydrogen atom, for example). However, when the dynamics is such that only two of them are occupied, one can consider only those two. For example $|0\rangle \equiv |1, 0, 0, 1/2\rangle$ and $|1\rangle \equiv |2, 1, 1, 1/2\rangle$;

  (b) Two Polarizations of A Photons: Consider a states of the electromagnetic field of a fixed wavevector $\vec{k}$ that contain one photon. There are two, corresponding to two polarizations. If the processes involving this flied do not change the frequency of the photons, one can describe them in terms of two levels, each of them corresponding two orthogonal polarizations of the photons;

  (c) Spin 1/2 Particle: An electron, proton, neuron, etc, has spin 1/2, and therefore can be describes as a two-level system.

1.2 States

1.2.1 Pure States

• General Pure States: The state of two-level system can be written as

$$|\Psi\rangle = c_0 |0\rangle + c_1 |1\rangle \tag{1.1}$$

where $c_{0,1}$ are complex numbers satisfying $|c_0|^2 + |c_1|^2 = 1$.
• Another Form: Without loss of generality, one can choose c_0 real and positive (since the state of Ψ does not depend on a global phase). Therefore, only two real variables determines any state. One can write

$$|\Psi\rangle = \cos\frac{\theta}{2} |0\rangle + e^{i\phi} \sin\frac{\theta}{2} |1\rangle , \tag{1.2}$$

where $\theta \in [0, \pi)$ and $\phi \in [0, 2\pi)$.
• Vector Form: Defining

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \equiv |0\rangle , \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv |1\rangle , \tag{1.3}$$

one can always write the state $|\Phi\rangle$ as

$$|\Phi\rangle = c_0 |0\rangle + c_1 |1\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \tag{1.4}$$

1.2.2 Mixed States

• General Form: Any state (pure or mixed) is described in terms of a density operator ρ. It can always be written as

$$\rho = q_{00} |0\rangle \langle 0| + q_{11} |1\rangle \langle 1| + q_{01} |0\rangle \langle 1| + q_{10} |1\rangle \langle 0| , \tag{1.5}$$

where q_{00} and $q - 11$ are real, positive numbers, and $q_{01} = q_{10}^*$ is a complex number. The properties of a density operator impose

$$q_{00} + q_{11} = 1, \quad q_{00}^2 + q_{11}^2 + 2|q_{01}|^2 \leqslant 1, \tag{1.6}$$

where the last one is consequence of $Tr(\rho^2) \leqslant 1$. It can also be written as $|q_{01}^2 \leqslant q_{00}q - 11$. Note that three real independent parameters characterize any mixed state (q_{00} and the real imaginary parts of q_{01}).
• Purity: The states (1.5) include the pure state. For the pure state (1.1) one has $q_{00} = |c_0|^2, q_{11} = |c_1|^2$, and $q_{01} = c_0 c_1^*$. Thus for pure states

$$|q_{01}|^2 = q_{00} q_{11} \tag{1.7}$$

.
• Operators: One can define

$$P_0 = |0\rangle \langle 0| , \quad \sigma_+ = |1\rangle \langle 0| \tag{1.8a}$$

,

$$P_1 = |1\rangle \langle 1| , \quad \sigma_- = |0\rangle \langle 1| \tag{1.8b}$$

. The first two are projectors (i.e., $P_i^2 = P_i$), whereas the second two are called excitation (σ_+) and deexcitation (σ_-) operators, respectively. The identity can be written as $I = P_0 + P_1$, and therefore one can express ant operator acting on the two-level system as a linear combination of these operators, in particular the density operator (1.5). According to (1.2), one can write them in the matrix for

$$P_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \sigma_+ = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

$$P_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_- = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

and therefore any operator can be expressed as a 2×2 matrix.
• Pauli operators: The operators (1.8) form a basis (they are linearly independent and any operator can be written as a linear superposition). Sometimes it is convenient to express them in terms of an *orthonormal basis*. To do that, one can has first to define a scalar product.
- Scalar Product: Let A and B be two operators acting on $\mathcal{H}_2$. We define the scalar product $(A, B) \equiv Tr(AB)$.
- Pauli Operators: We define the Pauli operators

$$\sigma_x = \sigma_+ + \sigma_- \tag{1.9a}$$

$$\sigma_y = -i(\sigma_+ - \sigma_-) \tag{1.9b}$$

$$\sigma_z = P_1 - P_0 \tag{1.9c}$$

- Commutation Relations: The Pauli operators satisfy angular momentum commutation relations:

$$[\sigma_x, \sigma_y] = 2i\sigma_z \tag{1.10a}$$

$$[\sigma_y, \sigma_z] = 2i\sigma_x \tag{1.10b}$$

$$[\sigma_z, \sigma_x] = 2i\sigma_y \tag{1.10c}$$

- Eigenvalues and Eigenstates: The Pauli operators are idempotent, $\sigma_i^2 = 1$, and therefore their eigenvalues are ±1. The eigenstates can be easily calculated:

$$\sigma_i |0\rangle_i = - |0\rangle_i , \sigma_i |1\rangle_i = |1\rangle_i , \tag{1.11}$$

where $i = x, y, z$, and

$$|0\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{1.12a}$$

$$|1\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{1.12b}$$

$$|0\rangle_y = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle) \tag{1.12c}$$

$$|0\rangle_y = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle) \tag{1.12d}$$

$$|0\rangle_z = |0\rangle \tag{1.12e}$$

$$|1\rangle_z = |1\rangle \tag{1.12f}$$

- Pauli Vector: One can define a Pauli vector $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. Defining a unit vector $\vec{n}$, one can define by $\vec{n}$ as $\sigma_{\vec{n}} = \vec{n} \cdot \vec{\sigma}$. This operator is also idempotent ($\sigma_{\vec{n}}^2 = 1$), and therefore has eigenvalues ±1. The corresponding eigenstates can be easily calculated.
- Basis: The set $A = A_i, i = 0, ..., 3 \equiv 1, \sigma_x.\sigma_y, \sigma_z$ is an orthonormal basis of the set of linear operators acting in $\mathrm{H}_2, \mathrm{L}(\mathrm{H}_2)$. That is, any linear operators can be written as a linear combination of the elements of the set, and this elements are mutually orthogonal (with the scalar product defined above).
- Matrix Form: Using the matrix form, we have

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \tag{1.13a}$$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.13b}$$

• Density Operator in Terms of Pauli Matrices: the density operator can be written as

$$\rho = \frac{1}{2}\sum_{i=0}^{3} \lambda_i A_i \tag{1.14}$$

where again $\{A_i\} \equiv \{1, \sigma_x, \sigma_y, \sigma_z\}$, and $\lambda_0 = 1$. Thus, any density operator can be described in terms of 3 real parameters and $\lambda_{1,2,3}$. In particular, we have $\lambda_i = Tr(\rho A_i)$, and according to (1.6),

$$\lambda_1^2 + \lambda_2^2 + \lambda_3^2 \leq 1 \tag{1.15}$$

The equality is fulfilled only for pure states [see (1.7)].
• Bloch Sphere: The form (1.14) together with the condition (1.15) suggests that one can represent graphically ant state as a vector in a sphere of unit radius, the Bloch sphere. In particular, using the Pauli vector $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$, and defining $\vec{\lambda} = (\lambda_1, \lambda_2, \lambda_3)$ we can write (1.14) as

$$\rho = \frac{1}{2}(1 + \vec{\lambda} \cdot \vec{\sigma}) \tag{1.16}$$

Thus, the state ρ is completely characterized by the vector $\vec{n}$ (one says that the state is "polarized" along the direction $\vec{n}$). Pure states are on the surface of the sphere, whereas mixed states are inside the sphere. Examples: $|1\rangle \to (0,0,1), |0\rangle \to (0,0,-1), \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \to (1,0,0)$.

1.3 Observables and Measurements

• Observables: Observables are self-adjoint operators $A = A^\dagger$. Any of these operators can be written in terms of the operators (1.8), since

$$\begin{aligned} O = 1O1 &= (P_0 + P_1)O(P_0 + P_1) \\ &= O_{00}\left|0\right\rangle\left\langle 0\right| + O_{11}\left|1\right\rangle\left\langle 1\right| + O_{01}\left|0\right\rangle\left\langle 1\right| + O_{10}\left|1\right\rangle\left\langle 0\right| \end{aligned} \tag{1.17}$$

Where $O_{ij} = \left\langle i\right| O \left|j\right\rangle = \left\langle j\right| O \left|i\right\rangle^*$. In a matrix form we can write

$$O = \begin{pmatrix} O_{00} & O_{10} \\ O_{01} & O_{11} \end{pmatrix} \tag{1.18}$$

Using the set A that includes that Pauli spin operators, we can also write

$$O = \frac{1}{2}\sum_{i=0}^{3} o_i A_i \tag{1.19}$$

where $o_i = Tr(OA_i)$.
• Measurements: Given an observable O, of eigenvalue $o_{1,2}$ and corresponding eigenstates $\left|\Phi_{1,2}\right\rangle$ (i.e. $O\left|\Phi_{1,2}\right\rangle = o_{1,2}\left|\Phi_{1,2}\right\rangle$), according to the postulates of Quantum Mechanics we have:
- Single Measurement: If the state of system is given by ρ, in a single measurement of O one obtains the result o_i with probability $P_i = \left\langle \Phi_i\right| \rho \left|\Phi_i\right\rangle, (i = 1, 2)$. If the measurement is a *filtering measurement*, after measuring o_i, the state of the system is projected (collapsed) onto $\left|\Phi_i\right\rangle$.
- Projectors: Any Projector P can be measured. If the result is 1, the state after the measurement is $P\rho P/Tr(P\rho P)$. If the result is 0, the state is $(1-P)\rho(1-P)/Tr[(1-P)\rho(1-P)]$.
- Expectation values: If one prepares a large number of systems in the same state described by ρ, and measures the observable O in all these systems, the averaged value is $\langle O\rangle = Tr(O\rho)$.
- State measurement: One cannot completely determine the state of a system, since the first measurement will give small information about it, and after the measurement the state is changed. If one is able to repeatedly prepare a system in a given state, then one can completely determine its state, that is, *rho*.

1.4 Unitary Evolution

• Schrödinger Equation: The evolution of a two-level system in a pure state is given by the Schrödinger equation

$$i\hbar\frac{\partial}{\partial t}\left|\Phi(t)\right\rangle = H(t)\left|\Phi(t)\right\rangle, \tag{1.20}$$

whereas, more generally, for a mixed state it is given by

$$i\hbar\frac{\partial}{\partial t}\rho(t) = [H(t), \rho(t)]\,, \tag{1.21}$$

where $H(t)$ is the Hamiltonian governing the dynamics.
• Hamiltonian: The Hamiltonian is an observable, so that we can write it as in (1.19),

$$H(t) = \frac{\hbar}{2}\sum_{i=0}^{3} h_i(t)A_i, \tag{1.22}$$

• Time-Independent Hamiltonian: In most of the cases of interest, H does not depend on time. Then, the exact evolution can be easily calculated. Ignoring the constant (c-number) term h_0, we can write the Hamiltonian (1.22) as

$$H = \hbar h \sigma_{\vec{n}}, \tag{1.23}$$

where $h = \sqrt{h_1^2 + h_2^2 + h_3^2}$, and $\vec{n} = (h_1, h_2, h_3)/h$ is a unit vector. The evolution operator $U(t) = e^{-iHt/\hbar}$ is given by

$$\begin{aligned} U(t) = e^{-ih\sigma_{\vec{n}}t} &= \cos h\sigma_{\vec{n}}t - i\sin h\sigma_{\vec{n}}t \\ &= \cos ht - i\sigma_{\vec{n}}\sin ht \end{aligned} \tag{1.24}$$

where we have used $\sigma_{\vec{n}}^2 = 1$.
• Euler Angles: Any unitary operation acting on a two-level system can be written in terms of the Euler angles (α, β, γ), and an irrelevant phase (δ).

$$U = U(\alpha, \beta, \gamma, \delta) = e^{-i\delta}e^{-i\alpha\sigma_x}e^{-i\beta\sigma_y}e^{-i\gamma\sigma_z} \tag{1.25}$$

• Quantum Optics: In quantum optics, one usually finds Hamiltonians written as

$$H = -\frac{\hbar\Delta}{2}\sigma_z + \frac{\hbar\Omega}{2}\left(\sigma_+ e^{-i\phi} + \sigma_- e^{i\phi}\right) \tag{1.26}$$

In this case we have $h = frac12\sqrt{\Omega^2 + \Delta^2}$ and

$$\sigma_{\vec{n}} = \frac{1}{\sqrt{\Omega^2 + \Delta^2}}\begin{pmatrix} -\Delta & \Omega e^{-i\phi} \\ \Omega e^{i\phi} & \Delta \end{pmatrix} \tag{1.27}$$

• Rabi Oscillations: For $\Delta = 0$, we have

$$U(t) = \begin{pmatrix} \cos\frac{\omega t}{2} & -i\sin\frac{\omega t}{2}e^{-i\phi} \\ -i\sin\frac{\omega t}{2}e^{i\phi} & \cos\frac{\omega t}{2} \end{pmatrix}. \tag{1.28}$$

If the system is prepared in $|1\rangle$, for example, the probability of finding it in $|1\rangle$ oscillates with a frequency Ω. These oscillations are called Rabi oscillations, and Ω is the Rabi frequency.

1.5 Decoherence

• Isolated Systems: Systems are never completely isolated. They interact with other degrees of freedom. what we call environment. The effects of these interactions is two fold: on the on hand, the system evolution is not the ideal one (nor even unitary); on the other hand, the state of the system becomes loss pure, and losses the coherences responsible for interference phenomena (decoherence).

• Interaction with The Environment: Consider a two-level system that it is coupled to the environment. Let us denote by $|E\rangle$ the initial state of the environment. The interaction of the system with the environment is in all generality described by a unitary operator, which can be characterized as follows:

$$|0\rangle \otimes |E\rangle \to |0\rangle \otimes |E_{00}\rangle + |1\rangle \otimes |E_{01}\rangle \tag{1.29a}$$

$$|1\rangle \otimes |E\rangle \to |0\rangle \otimes |E_{10}\rangle + |1\rangle \otimes |E_{11}\rangle \tag{1.29b}$$

where $|E_{ij}\rangle$ are unnormalized states of the environment. Unitary imposes

$$\langle E_{00}|E_{00}\rangle + \langle E_{01}|E_{01}\rangle = 1 \tag{1.30a}$$

$$\langle E_{10}|E_{10}\rangle + \langle E_{11}|E_{11}\rangle = 1 \tag{1.30b}$$

$$\langle E_{00}|E_{10}\rangle + \langle E_{01}|E_{11}\rangle = 0 \tag{1.30c}$$

• Reduced Density Operator: Since we cannot measure all the degrees of freedom of the environment, all the information of the system will be in the reduced density operator defined after tracing over the environment degrees of freedom. If the initial state of the system was

$$|\psi_0\rangle = c_0 |0\rangle + c_1 |1\rangle \tag{1.31}$$

after the interaction with environment, the state will be

$$\begin{aligned} |\psi(t)\rangle = {} & c_0 \left(|0\rangle \otimes |E_{00}\rangle + |1\rangle \otimes |E_{01}\rangle\right) \\ & + c_1 \left(|0\rangle \otimes |E_{10}\rangle + |1\rangle \otimes |E_{11}\rangle\right) \\ & = |0\rangle \left(c_0 |E_{00}\rangle + c_1 |E_{10}\rangle\right) + |1\rangle \left(c_0 |E_{01}\rangle + c_1 |E_{11}\rangle\right) \end{aligned}$$

Tracing over the state of the environment, we get

$$\begin{aligned} \langle 0| \rho |0\rangle = {} & |c_0|^2 \langle E_{00}|E_{00}\rangle + |c_1|^2 \langle E_{01}|E_{01}\rangle \\ & + c_0^* c_1 \langle E_{00}|E_{01}\rangle + c_1^* c_0 \langle E_{01}|E_{00}\rangle , \end{aligned} \tag{1.32a}$$

$$\begin{aligned} \langle 0| \rho |1\rangle = {} & |c_0|^2 \langle E_{01}|E_{00}\rangle + |c_1|^2 \langle E_{11}|E_{10}\rangle \\ & + c_0^* c_1 \langle E_{01}|E_{10}\rangle + c_1^* c_0 \langle E_{11}|E_{00}\rangle , \end{aligned} \tag{1.32b}$$

and $\langle 1| \rho |1\rangle = \mathbf{1} - \langle 0| \rho |0\rangle , \langle 1| \rho |0\rangle = \langle 0| \rho |1\rangle^*$. Thus the state of the system changes due to the coupling to the environment.

• Purity: In general, the state of the system will not be pure anymore. Consider the simple case where $|E_{01}\rangle = |E_{10}\rangle = 0$, and with $c_0 = c_1 = 1/\sqrt{2}$. Thus,

$$\rho = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| + |0\rangle\langle 1| \langle E_{11}|E_{00}\rangle + |1\rangle\langle 0| \langle E_{00}|E_{11}\rangle) \tag{1.33}$$

If $\langle E_{11}|E_{00}\rangle = 0$, the coherences disappear in the density operator, and therefore the state becomes impure [the purity $Tr(\rho^2)$ goes down to 1/2]. This is what in reality occurs: due to the interaction with the environment, $\langle E_{11}|E_{00}\rangle \to e^{-\gamma t}$, so that after a time $\tau_c \simeq 1/\gamma$ the quantum behavior is lost. The time τ_c is called *decoherence time*.

Chapter 2

COMPOSITE TWO-LEVEL SYSTEM

2.1 Generalities

• Composite Two-level Systems: We consider 2 or more two-level systems. Most of the time we will restrict ourselves 2 two-level systems, A and B.
• Hilbert Space: the Hilbert space describing the whole problem is $\mathcal{H}_4 = \mathcal{H}_2 \otimes \mathcal{H}_2$. A basis in this Hilbert space is $\{|0\rangle_A \otimes |0\rangle_B, |0\rangle_A \otimes |1\rangle_B, |1\rangle_A \otimes |0\rangle_B, |1\rangle_A \otimes |1\rangle_B\}$.
• Physical Situations: One can have these systems in several physical contexts. For example, two atoms, two modes, two electrons, etc.
• Entanglement: The most important quantum property of composite two-level systems is entanglement.

2.2 States

2.2.1 Pure States

• Pure states: Pure states can be written in the basis defined above:

$$\begin{aligned} |\Psi\rangle =& c_{00} |0\rangle_A \otimes |0\rangle_B + c_{01} |0\rangle_A \otimes |1\rangle_B \\ &+ c_{10} |1\rangle_A \otimes |0\rangle_B + c_{11} |1\rangle_A \otimes |1\rangle_B \end{aligned} \tag{2.1}$$

where the c's are complex numbers satisfying $|c_{00}|^2 + |c_{01}|^2 + |c_{10}|^2 + |c_{11}|^2 = 1$. Now, 6 independent parameters characterize a state in $\mathcal{H}_4$. In the following we will not write explicitly the symbols $\otimes$, and sometimes we will the shorthand notation $|00\rangle = |0\rangle_A |0\rangle_B$, or even binary notation (for example $|3\rangle = |11\rangle$).

• Vector Form: One can write the basis states in a vector form

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \equiv |0\rangle_A |0\rangle_B = |0\rangle , \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \equiv |0\rangle_A |1\rangle_B = |1\rangle ,$$

$$\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \equiv |1\rangle_A |0\rangle_B = |2\rangle , \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \equiv |1\rangle_A |1\rangle_B = |3\rangle ,$$

Thus, any state can be written as a (complex) vector.
• Reduced density operator: Suppose one is interested only in one of the subsystems, say A. Since the other system is not measured, the state of A will be obtained as the partial trace of the state of the whole system.

$$\rho_A = Tr_A \left(|\Psi\rangle \langle\Psi| \right), \rho_B = Tr_B \left(|\Psi\rangle \langle\Psi| \right), \tag{2.2}$$

Despite the fact that $|\Psi\rangle$ is a pure state, ρA and ρ_B may describe mixed states. In fact, for any mixed state ρ_A of a two-level system, one can always find a pure state $|\Psi\rangle$ of a composite system such that $\rho_A \equiv Tr_A \left(|\Psi\rangle \langle\Psi| \right)$.
• Uncorrelated States: Those are states of the form $|\Psi\rangle = |\Psi_1\rangle_A \otimes |\Psi_2\rangle_B$. That is they are states that can be factored.
- General form: Denoting $|\Psi_1\rangle_A = c_0^A |0\rangle_A + = c_1^A |1\rangle_A$, and $|\Psi_2\rangle_B = c_0^B |0\rangle_B + = c_1^B |1\rangle_B$, uncorrelated states are of the form

$$\begin{pmatrix} c_{11} \\ c_{10} \\ c_{01} \\ c_{00} \end{pmatrix} = \begin{pmatrix} c_1^A c_1^B \\ c_1^A c_0^B \\ c_0^A c_1^B \\ c_0^A c_0^B \end{pmatrix} . \tag{2.3}$$

Thus, they satisfy

$$c_{00} c_{11} = c_{01} c_{10} \tag{2.4}$$

Therefore, they are determined by 4 real parameters, they are a (zero measure) subset in $\mathcal{H}_4$.
-Basis: Uncorrelated states do not form a subspace of $\mathcal{H}_4$. However, one can find a basis in $\mathcal{H}_4$ form by uncorrelated states. An example is the basis taken at the beginning of this Section.
- Reduced density operator: For uncorrelated states, the reduced density operators have the trivial form $\rho_A = |\Psi_1\rangle_A \langle\Psi_1| , \rho_B = |\Psi_2\rangle_B \langle\Psi_2|$.
• Entangled States: Entangled states are those that cannot be written as product states $|\Psi\rangle = |\Psi_1\rangle_A \otimes |\Psi_2\rangle_B$. For example, the *singlet state*

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B \right). \tag{2.5}$$

- Most states are entangled: Note that ”most” states are entangled (mathematically, the set entangled states is dense in $\mathcal{H}_4$).
- Basis: One can find basis in $\mathcal{H}_4$ formed by entangled states. For example, the so-called Bell states:

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_A |1\rangle_B \pm |1\rangle_A |0\rangle_B \right) \tag{2.6a}$$

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_A |0\rangle_B \pm |1\rangle_A |1\rangle_B \right) \tag{2.6b}$$

- Maximally entangled states: Those are states that can be obtained from one of the elements of the Bell basis by applying a different unitary operation to each of the subsystems, independently.
- GHZ states: Of particular interest are the state of N two-level system of the form

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle |0\rangle ... |0\rangle - |1\rangle |1\rangle ... |1\rangle \right) \tag{2.7}$$

These are highly entangled states.
• Schmidt decomposition: Given two systems A and B is a pure state $|\Psi\rangle$ it is always possible to write this state as

$$|\Psi\rangle = \sum_j \lambda_j |u_j\rangle_A |v_j\rangle_B, \tag{2.8}$$

where $\langle u_i | u_j \rangle = \langle v_i | v_j \rangle = \delta_{i,j}$. The from (2.8) is called Schmidt decomposition. The reduced density operators for both systems can therefore be written as

$$\rho_A = \sum_j |\lambda_j|^2 |u_j\rangle_A \langle u_j| \tag{2.9a}$$

$$\rho_B = \sum_j |\lambda_j|^2 |v_j\rangle_B \langle v_j| \tag{2.9b}$$

2.2.2 Mixed States

• Mixed Stated: All the states (pure or mixed) can be described in terms of a density operator. In the basis (2.2), one has

$$\rho = \sum_{i,j=0}^{3} \rho_{i,j} |i\rangle_{AB} \langle j|, \tag{2.10}$$

which can be written as a 4×4 matrix. The coefficients $\rho_{i,j}$ must be such $\rho = \rho^\dagger$. $\mathrm{Tr}(\rho) = 1$ and $\rho^2 < \rho$.

• Pauli Operators: Defining the set of operators

$$\begin{aligned}\{A_i|i\ from\ 0\ to\ 15\} =&\{1, \sigma_x^B, \sigma_y^B, \sigma_z^B, \sigma_x^A\sigma_x^B, \sigma_x^A\sigma_y^B, \sigma_x^A\sigma_z^B,\\ &\sigma_y^A\sigma_x^B, \sigma_y^A\sigma_y^B, \sigma_y^A\sigma_z^B, \sigma_z^A\sigma_x^B, \sigma_z^A\sigma_y^B, \sigma_z^A\sigma_z^B\}\end{aligned}$$

one can write

$$\rho = \frac{1}{4}\sum_{i=0}^{15} \lambda_i A_i \tag{2.11}$$

where λ_i are real coefficients ($\lambda_0 = 1$). Thus, a density operator is characterized by 15 real parameters. Note that $\lambda_i = \mathrm{Tr}(\rho A_i)$.

• Uncorrelated States: Those are states whose density operator can be written as $\rho = \rho_A \otimes \rho_B$, where $\rho_{A,B}$ are density operators of the first and second subsystem. For these states, the reduced density operators coincide with ρ_A and ρ_B, respectively.

• Separable States: Those are states that can be written as sums of uncorrelated states, i.e.

$$\rho = \sum_k P_k \rho_A^k \otimes \rho_B^k \tag{2.12}$$

• Inseparable States: Those are states that cannot be written in the form (2.12). For example, the state

$$\rho = f\left|\Psi^+\right\rangle\left\langle\Psi^+\right| + (1-f)\left|\Phi^+\right\rangle\left\langle\Phi^+\right|, \tag{2.13}$$

with $f \leq 1$.

• Separability Criterion: A given density operator ρ describing the state of 2 two-level systems is separable if and only if the partial transpose operator with respect to any of the subsystems is positive definite (has no negative eigenvalues). Writing

$$\begin{aligned}\rho =& {}_A\langle 0|\rho|0\rangle_A\,|0\rangle_A\langle 0| + {}_A\langle 1|\rho|1\rangle_A\,|1\rangle_A\langle 1|\\ &+ {}_A\langle 0|\rho|1\rangle_A\,|0\rangle_A\langle 1| + {}_A\langle 1|\rho|0\rangle_A\,|1\rangle_A\langle 0|.\end{aligned} \tag{2.14}$$

the partial transpose of a density operator with respect to the system A is obtained as

$$\begin{aligned}\rho^{T_A} =& {}_A\langle 0|\rho|0\rangle_A\,|0\rangle_A\langle 0| + {}_A\langle 1|\rho|1\rangle_A\,|1\rangle_A\langle 1|\\ &+ {}_A\langle 0|\rho|1\rangle_A\,|1\rangle_A\langle 0| + {}_A\langle 1|\rho|0\rangle_A\,|0\rangle_A\langle 1|.\end{aligned} \tag{2.15}$$

One can show that this is equivalent to exchanging $\sigma_y^A \to -\sigma_y^A$ in (2.11).

2.3 Observables And Measurements

• Reduced Density Operators: As in the case of pure state, one can define the reduced density operators

$$\rho_A = Tr_A(\rho) \quad \rho_B = Tr_B(\rho) \tag{2.16}$$

• Observables: Observables are self-adjoint operators $O = O^\dagger$. THey can be written as 4×4 matrices in a basis set [for example, in (2.2) or (2.6)]. Alternatively, they can be written as

$$O = \frac{1}{4}\sum_{i=0}^{15} o_i A_i, \tag{2.17}$$

where $o_i = Tr(OA_i)$.
• Measurements: The probabilities, expectation values, etc of measurements of an observable O can be calculated in terms of ρ. - Local measurements: If a measurement is performed on system A only, this is called a local measurement on A. For example, if one measures the observable $O = O_A \otimes I_B$ this would correspond to a local measurement in A. All the results of such measurements can be determined by the reduced density operators. The reason is that $Tr(\rho O) = Tr_A\left[Tr_B(\rho O)\right] = Tr_A\left[Tr_B(\rho) O_A\right] = Tr_A(\rho_A O_A)$.
- Correlation measurements: One can perform simultaneous local measurements in A and B and compare the corresponding result. For example, if one measures O_A in system A and O_B in system B, and multiply the corresponding results, this is equivalent to measure the observable $O = O_A O_B$. Note that only for uncorrelated states $\langle O\rangle = \langle O_A\rangle \langle O_B\rangle$.
- Joint measurements: These are measurements that not performed locally, i.e. they do not correspond to observables $O = O_A O_B$. For example, $O = \sigma_x^A \sigma_y^B + \sigma_y^A \sigma_x^B$. An important example consists of the so-called measurements in the Bell Basis. The correspond to the measurement of an observable whose eigenstates are the Bell states, so that as a result of measurement one of the Bell States is found (or equivalently, to measure the 4 projectors onto the Bell basis states.)
• POVM: Suppose we have a system in a state ρ. We can perform measurements by taking ab auxiliary system (usually called ancilla) in a known state ρ_A, and measure in the joint system a set of orthogonal projector operators P_μ (with $\sum_\mu P_\mu = 1$). As a result of the measurement we will obtain one of the P_μ. The probability of obtaining a particular projector in a single measurement is

$$\begin{aligned} p_\mu &= Tr(P_\mu \rho \otimes \rho_a) \\ &= \sum_{m,n=0}^{1} \sum_{r,s} (P_\mu)_{mr,ns} (\rho)_{nm} (\rho_a)_{sr} \\ &= \sum_{m,n=0} 1 \, (A_\mu)_{nm} (\rho)_{nm} = Tr(A_\mu \rho) \end{aligned} \tag{2.18}$$

where

$$(A_\mu)_{nm} = \sum_{r,s} (P_\mu)_{mr,ns} (\rho_a)_{sr}. \tag{2.19}$$

The set of operators A_μ is called a *positive operator valued measurement*(POVM), since the A_μ are positive (since the trace of A_μ with positive operators ρ are always positive). They are also hermitian, and

$$\sum_\mu A_\mu = 1. \tag{2.20}$$

It can be showed (Neumark's theorem) that there always exists a physical mechanism (i.e. interaction with an ancilla) that generates ant desired POVM represented by given matrices A_μ hermitian, positive, and fulfilling (2.20). Measurements of POVM on a system are the most general measurements one can perform.

2.4 Unitary Evolution

• Schrödinger Equation: The evolution of a two-level system in a pure state is given by the Schrödinger Equation

$$i\hbar \frac{\partial}{\partial t} |\Psi(t)\rangle = H(t) |\Psi(t)\rangle , \tag{2.21}$$

whereas for a mixed state it is given by

$$i\hbar \frac{\partial}{\partial t} \rho(t) = [H(t), \rho(t)], \tag{2.22}$$

where $H(t)$ is the Hamiltonian.
• Hamiltonian: The Hamiltonian is an observable, so that we can write is as in (2.17),

$$H(t) = \hbar \frac{1}{2} \sum_{i=0}^{15} h_i(t) A_i. \tag{2.23}$$

• Local interactions: Those are interactions corresponding to Hamiltonians of the form $H = H_A + H_B$, where H_A and H_B only act on the systems A and B, respectively. In that case, since $[H_A, H_B] = 0$, one can write $U(t) = U_A(t)U_B(t)$, where $U_{A,B}$ are the evolution operators for the system A and B. A local evolution cannot entangle two systems, if they are initially untangled. Similarly, it cannot disentangle two systems that are initially entangled.
• Nonlocal interactions: These interactions can entangle two initially unentangled systems. Foe example, $H = \hbar\alpha\sigma_x^A\sigma_y^B$ gives the evolution operator:

$$U(t) = \cos\alpha t - i\sigma_x^A\sigma_y^B \sin\alpha t, \tag{2.24}$$

for $\alpha t = \pi/4$, the evolution of the state $|0\rangle_A |0\rangle_B$ is

$$U(t) |0\rangle_A |0\rangle_B = |\Phi^-\rangle \,, \tag{2.25}$$

i.e. corresponds to the preparation of a bell state.

• No Cloning Theorem: States cannot be cloned (copied). This can be proved as follows. Imagine we want to copy an unknown state of one two-level system $|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle$, to another two-level system, prepared in the known state $|\psi_0\rangle$. Thus, we have to find an unitary transformation such that

$$U |\psi\rangle |\psi_0\rangle = |\psi\rangle |\psi\rangle \tag{2.26}$$

for any $|\psi\rangle$. Take two cases $|\psi_1\rangle$ and $|\psi_2\rangle$. Using (2.26) for both of them, and using the fact that any unitary operator conserves the scalar product we deduced that $\langle\psi_1|\psi_2\rangle < \langle\psi_1|\psi_2\rangle^2$ which is always false unless $\langle\psi_1|\psi_2\rangle = 0, 1$. Thus, only states that are orthogonal can be copied.

• Swapping: The swapping operation defined as

$$U |\psi_1\rangle |\psi_0\rangle = |\psi_0\rangle |\psi_1\rangle \tag{2.27}$$

does not violate any rule of quantum mechanics.

2.5 Decoherence

• Interaction with the environment: When one has more than one system, the interaction with the environment becomes more critical.

• Simple model of environment: Consider N two-level system, each of them interacting with its own environment. we denote by $|E^i\rangle$ the initial state of the environment for system i, and assume the following evolution

$$|0\rangle_i \otimes |E^i\rangle \to |0\rangle_i \otimes |E^i_{00}\rangle \tag{2.28a}$$

$$|1\rangle_i \otimes |E^i\rangle \to |1\rangle_i \otimes |E^i_{11}\rangle \tag{2.28b}$$

where $\langle E^i_{00}|E^i_{00}\rangle = 1, \langle E^i_{11}|E^i_{11}\rangle = 1$, and $\langle E^i_{00}|E^i_{11}\rangle = e^{-\gamma t}$.

• Reduced density operator: If initially one system prepared all two-level systems in the state $(|0\rangle_i + |1\rangle_i)/sqrt2$, after a time t the reduced density operator will be of the form

$$\langle a_1, a_2, ..., a_N| \, \rho \, |b_1, b_2, ...b_N\rangle = \frac{1}{2^N} e^{-\gamma t H(\vec{a},\vec{b})},$$

where $a_i = 0, 1, b_i = 0, 1$, and $H(\vec{a},\vec{b})$ is the Hamming distance between the vectors $\vec{a}$ and $\vec{b}$. This distance is defined as the number of instances in which $a_i \neq b_i$. In particular, the coherence

$$\langle 0,0,...,0|\,\rho\,|1,1,...,1\rangle = \frac{1}{2^N} e^{-\gamma N t}, \tag{2.29}$$

i.e. it decays much faster than for the single two-level system. If one is looking at an interference phenomena in which this matrix element is important, the interaction with the environment will destroy the interference pattern.

Chapter 3

ENTANGLEMENT AND NONLOCALITY

3.1 Einstein-Podolsky-Rosen Paradox

• Entangled States raised controversy in the 30's. The maximum exponent was the article of Einstein, Podolsky, and Rosen (EPR) "Can Quantum Mechanical description of physical reality be considered complete?". In that article they show, using a paradox, that Quantum Mechanics cannot give a complete description of a system.
• Elements Of Reality: If, without in any way disturbing a system, we can predict with certainty the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity. This means that this physical quantity has a value independently of whether we measure it or not.
• Single State: Consider the singlet state of two particles (two-level systems) A and B,

$$|\Psi\rangle = \frac{1}{2}\left(|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B\right) \tag{3.1}$$

These systems are separated by a long distance L, such that at the time of measurement the two systems do not interact; therefore, no real change can take place in the second system in consequence of anything that may be done to the first system.
• Measurements: Suppose A and B measure the state of their respective particles.
- σ_z: First consider the case where they measure the observable σ_z. We denote by m_z^a and m_z^b the results of the measurements. If $m_z^a = 1$ then m_z^b *has to be* $m_z^b = -1$. On the other hand, If $m_z^a = -1$ then $m_z^b = 1$. In other words, if one measures σ_z^a in particle A, the result of σ_z^b for the second particle is completely determined without disturbing it. Thus σ_z^b is an element of reality, i.e. has to be determined whether one measures or not.
- σ_x: Now consider the case where they measure the observable σ_x is measured.

We denote by m_x^a and m_x^b the results of the measurements. If $m_x^a = 1$ then m_x^b *has to be* $m_x^b = -1$. This is so because ${}_A\langle 1_x|\Psi\rangle = \frac{1}{\sqrt{2}}(|1\rangle_B - |0\rangle_B)$, which is precisely $|0_x\rangle_B$. On the other hand, If $m_x^a = -1$ then $m_x^b = 1$.If one measures σ_z^a in particle A, σ_x^b is completely determined without disturbing the second particle. Thus σ_z^b is an element of reality.
- σ_y: Analogously, σ_y^b is an element of reality.
• Paradox: $\sigma_{x,y,z}^B$ are elements of reality, i.e. they are well define before a measurement. However, according to quantum mechanics, one cannot know the value of three observables simultaneously, since the corresponding operators do not commute.
• What is Wrong With QM?: According to Einstein, "it becomes evident that the paradox forces us to relinquish one of the following assertions: (1) the description by means of a wavefunction is not complete; (2) the real states of spatially separated systems are not dependent". According to Einstein, the second assertion is indisputable since "the situation of system B is independent of what is done with system A, which is spatially separated from the former". This physical principle has received the name Einstein locality.
• Bohr Response: Bohr answered that the experiments used to determine m_x, m_y and m_z are different, so that no conclusions can be made about elements of reality. The possible outcomes depend on what is measured.
• Hidden Variables: According to Einstein, hidden variables are needed to complete QM. THese are variables that cannot be measured (at least in principle), and that determine the result of any particular experiment. If one averages statistically over the possible values of the hidden variables, one would obtain the same results as the expectation values of QM. A *realist theory* is that which assumes that the observables (elements of reality) can be described by a set of hidden variables.

3.2 Bell Theorem

Bell proved that if one assumes the validity of Einstein locality, Quantum Mechanics is not compatible with the existence of hidden variables. That is, any theory which is based on hidden variables (i.e. realist theory) as well as on locality will give a different result that the one predicted by Quantum Mechanics for some given experiments.

3.2.1 Gedamken Experiment

• Imagine the situation in which pairs of distant particles are in the EPR singlet state (3.1). The observable $\sigma_{\vec{a}}$ is measured in system A and $\sigma_{\vec{b}}$ in B. The results of measurements would fulfill the following properties:
- Measurement in A. If one measures the observable $\sigma_{\vec{a}} \equiv \vec{\sigma} \times \vec{a}$ in system A, one can obtain two values, $m_{\vec{a}} = \pm 1$.
- Measurement in B. Analogously, if one measures the observable $\sigma_{\vec{b}} \equiv \vec{\sigma} \times \vec{b}$ in system B, one can obtain two values, $m_{\vec{b}} = \pm 1$.

- Correlations: If one measures on the same pair $\sigma_{\vec{a}}$ and $\sigma_{\vec{b}}$ the results will be uncorrelated. That is, $m_{\vec{a}}m_{\vec{b}} = -1$.

3.2.2 Analysis: Hidden variables theory. Bell Inequality

• Hidden Variables: Let us describe the above experiment assuming the existence of hidden variables. We therefore assume that the outcome of each single realization of any experiment depends on a set of hidden variables λ, which change from experiment to experiment. This set of variables are distributed statistically according to an unknown distribution $\rho(\lambda) \geq 0$, which is normalized to one.
• Experiment: A *realist theory* imposes that the results of the measurements in a given single realization of the experiment depend on $\vec{a}, \vec{b}$, and on a set of hidden variables λ, which change from experiment to experiment. Moreover, the following properties must be fulfilled:
- Measurement In A: We can write that the result when measuring $\sigma_{\vec{a}}$, A, is a function of a and λ, and takes on the values ± 1, that is $A = A(\vec{a}, \lambda) = \pm 1$. The fact that the result if this experiment does not depend on $\vec{b}$ is due to *Einstein locality.*
- Measurement In B: Similarly, the result when measuring $\sigma_{\vec{b}}$, $B = B(\vec{b}, \lambda) = \pm 1$.
- Correlations: There is perfect anti-correlation, that is $A(\vec{a}, \lambda)B(\vec{b}, \lambda) = -1$.
• Expectation Values: If we perform several times the experiments for given $\vec{a}$ and $\vec{b}$, multiply $A(\vec{a}, \lambda)B(\vec{b}, \lambda)$ each time, and average over all the experiments, we will obtain the result

$$E(\vec{a}, \vec{b}) = \int d\lambda \rho(\lambda) A(\vec{a}, \lambda) B(\vec{b}, \lambda). \tag{3.2}$$

where $\rho\lambda$ is the statistical distribution of the hidden variables, which is unknown. In the same way, if we run another set of experiments choosing other directions we will have similar expressions for $E(\vec{a}, \vec{c})$ and $E(\vec{b}, \vec{c})$.

$$\begin{aligned} E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{c}) &= \int d\lambda \rho(\lambda) \left[A(\vec{a}, \lambda) B(\vec{b}, \lambda) - A(\vec{a}, \lambda) B(\vec{c}, \lambda) \right] \\ &= -\int d\lambda \rho(\lambda) \left[1 + A(\vec{a}, \lambda) B(\vec{c}, \lambda) \right] \end{aligned}$$

where we have used that $A(\vec{b}, \lambda)^2 = 1$, and that $B(\vec{b}, \lambda) = -A(\vec{b}, \lambda)$. Calculating the modulus, and taking into account that $|A(\vec{a}, \lambda)A(\vec{b}, \lambda)| = 1$, we find the Bell inequality.
• Bell Inequality:

$$|E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{c})| \leq 1 + E(\vec{b}, \vec{c}). \tag{3.3}$$

This inequality is predicted by ant local realist theory in any experiment as the one described above.

3.2.3 Analysis: Quantum Mechanics

• Expectation Values: If one performs many times experiments with pair of particles in the state (3.1), and for each pair of experiments one calculates the product $m_{\vec{a}} m_{\vec{b}}$, according to QM, the result will be $E(\vec{a},\vec{b}) = \langle\Psi|\, \sigma_{\vec{a}}\sigma_{\vec{b}}\, |\Psi\rangle = -\cos{(\vec{a}\cdot\vec{b})}$. Note that if $\vec{b}=\vec{a}$, then in all the experiments $m_{\vec{a}} m_{\vec{b}} = -1$, as we have been in the previous section.
• Violations of Bell Inequality: QM violates Bell inequalities. Simply select the $\angle\vec{a},\vec{b} = \angle\vec{b},\vec{c} = \pi/3$ and $\angle\vec{a},\vec{c} = 2\pi/3$. In that case $E(\vec{a},\vec{b}) = E(\vec{b},\vec{c}) = 1/2, E(\vec{a},\vec{c}) = -1/2$. Bell inequality (3.3) would give $1 \leq 1/2$. This proves Bell theorem, and therefore QM is incompatible with local realist theories. An experimental test can decide which one is wrong.

3.3 CHSH Inequalities

• Generalization: Bell inequalities can be generalized. For example, imagine that in some of the measurements the detectors (measurement apparatus) fail. In this case, one can assign a value 0 to A or B. Also, it may happen that the anticorrelation assumed in the derivation of Bell's theorem is not perfect since the EPR pair is not precisely prepared. Clauser, Horne, Shimony and Holt derived an inequality which takes all this into account.
•Assumptions: Let us assume that

$$E(\vec{a},\vec{b}) = \int d\lambda \rho(\lambda) A(\vec{a},\lambda) B(\vec{b},\lambda). \tag{3.4}$$

where the only requirement is $|A||B| \leq 1$.

$$\begin{aligned} E(\vec{a},\vec{b}) - E(\vec{a},\vec{c}) &= \int d\lambda\rho(\lambda)\left[A(\vec{a},\lambda)B(\vec{b},\lambda) - A(\vec{a},\lambda)B(\vec{c},\lambda)\right] \\ &= \int d\lambda\rho(\lambda)A(\vec{a},\lambda)B(\vec{b},\lambda)\left[1 \pm A(\vec{d},\lambda)B(\vec{c},\lambda)\right], \\ &- \int d\lambda\rho(\lambda)A(\vec{a},\lambda)B(\vec{c},\lambda)\left[1 \pm A(\vec{d},\lambda)B(\vec{b},\lambda)\right]. \end{aligned}$$

Using $|A|, |B| \leq 1$, we have

$$|E(\vec{a},\vec{b}) - E(\vec{a},\vec{c})| \leq 2 \pm |E(\vec{d},\vec{c}) + E(\vec{d},\vec{b})|. \tag{3.5}$$

This inequality has to be fulfilled by any local realist theory. For the particular case $\vec{d} = \vec{c}$ and $E(\vec{c},\vec{c}) = -1$, it reduces to Bell inequality (3.3).
• Violations of The CHSH Inequality: Take the quantum mechanical prediction for $\angle\vec{a},\vec{b} = \angle\vec{b},\vec{d} = \angle\vec{d},\vec{c} = \pi/4$, which gives $E(\vec{a},\vec{b}) = E(\vec{b},\vec{d}) = E(\vec{d},\vec{c}) = -1/\sqrt{2}$, $E(\vec{a},\vec{c}) = 1/\sqrt{2}$. We find $S = 2\sqrt{2} > 2$.

• Other Generalizations: There are other generalizations, which are best suited for experiments. For example, the Clauser-Horn (CH) inequality:

$$P_{12}(\vec{a},\vec{b}) - P_{12}(\vec{a},\vec{c}) + P_{12}(\vec{d},\vec{b}) + P_{12}(\vec{d},\vec{c}) \leq P_1(\vec{d}) + P_2(\vec{c}), \tag{3.6}$$

where P_{12} denotes the coincidence probability (i.e. probability of detecting either +1 in both systems A and B or -1) and P_1 and P_2 the probability of detecting in system 1 and 2, respectively.

Chapter 4

Quantum Communication and Computation

4.1 Cryptography

• Goal: the goal of classical cryptography is the secret communication. That is, a *sender* (whom we will call Alice) wants to transmit a secret message to a *received* (Bob). This transmission has to be such that any Eavesdropped (Eve) does not capture the message.
• Traditional Methods: Cryptographic methods are known since long ago. For example, the Spartans used a simple transposition methods to send secret messages, whereas Romans used substitution methods.
- Transposition: It consists of changing the place (transposing) the letter that compose the message. For example, one can exchange consecutive letters: COLD→OCDL.
- Substitution: It consists of changing the order of the letter that compose the alphabet. For example, A→D, B→E, C→F, etc. In this case, COLD→FROG.
- Security: This methods are not secure. For example, it is well known that the frequency of appearance of a given letter in any intelligible text is more or less constant. This means that if Eve takes the message (which is suppose to be long) and compares the relative frequency appearance of the signs with the standard tables, she can decode the message.
• ONE-TIME PAD: In 1917 a cryptographic scheme was proposed, which is provably secure (i.e., unbreakable). The ideas is that Alice and Bob, prior to the transmission, have a *key*, which nobody else knows. This key is a random sequence of numbers K_1, K_2,... The procedure is as follows: Alice takes her message and encrypts it using the key. TO do that, she uses first a public table to translate the letters of the message to numbers, P_1, P_2... The encrypted message is obtained by adding P and K modules N, the number of letters in the alphabet, i.e. $C_i = P_i + K_i \text{mod}(N)$. She sends the encrypted message C to Bob, who decrypts it using the key, as $P_i = C_i - K_i \text{mod}(N)$. Since the key is

random, for somebody who does not know the key, C_i are completely random. It can be proved that if the length of key is the same as the length of the message, and a given key is only used once and then discarded, this procedure is secure.

• Example: Let us take the public table:

A	B	C	D	...	Y	Z		?	,	.
01	02	03	04	...	25	26	27	28	29	30

in this case, $N = 30$. The random secret key is

12	01	18	27	03	23	05	10	21	24	...

The word UNIVERSITY will be encrypted as

U	N	I	V	E	R	S	I	T	Y
21	14	09	22	05	18	19	09	20	25
12	01	18	27	03	23	05	10	21	24
03	15	27	19	08	01	24	19	11	19

• Problem: THe problem is that Alice and Bob have to know the key in advance, and therefore they have to communicate to establish this key. This process is called *distribution*. In principle, there are two ways of achieving that, but non of them is completely secure.

- Use physical communication means: These means cannot be always secure.
- Use mathematical methods: Public key cryptography was introduced in 1976. It is based on the existence of mathematical operations that are easy to perform, but whose inverse are difficult. For example, it is simple to multiply two numbers ($127 \times 229 = ?$) but it is difficult to decompose a number in prime factors ($29083 = ? \times ?$). The idea is that Alice knows how to perform two mutually inverse transformations (a scrambling transformation and an unscrambling transformation). Then she publishes the directions (recipe) for performing the scrambling transformation, so that anybody can use this recipe to encode a message, but she is the only one who can perform the inverse transformation. This method is based in unproved mathematical assumption (i.e. that the time required to find the prime factors of a given number of size n with a computer scales as an exponential function of n).

4.2 Quantum Cryptography: Quantum Public Key Distribution

Idea: Instead of using for public key distribution a mathematical difficulty of a particular computation, use a physical law that prevents eavesdropping. This law is related to quantum mechanics: if Eve tries to measure the unknown state of a system, she will always perturb the state, so that Alice and Bob can know that their communication is not secure.

4.2.1 BB84 Protocol

• Goal: The goal for Alice and Bob is to share a random key. The key is a long sequence of random bits.
• Procedure:
(1) *Preparation and transmission*: Alice prepares a set of two-level systems (quantum bits, or in short qubits) in states chosen randomly among the set $S = \{|0\rangle_x, |1\rangle_x, |0\rangle_z, |1\rangle_z\}$, where $|0\rangle_x, |1\rangle_x$ are the eigenstate of the σ_x operator, and $|0\rangle_z, |1\rangle_z\}$ are the eigenstate of σ_z. That is,

$$|1\rangle_x = \frac{1}{2}(|0\rangle_z + |1\rangle_z), \quad |0\rangle_x = \frac{1}{2}(|0\rangle_z - |1\rangle_z). \tag{4.1}$$

She sends these qubits to Bob.
(2) *measurement*: For each of the qubits received, Bob chooses randomly among z and x, and correspondingly he measures either σ_x or σ_z.
(3) *Public discussion*: Bob announces publicly the operator he has measured for each of the qubits, without saying the outcome of the measurement. Then, Alice announces publicly for each qubit if the operator that Bob has measured corresponds to the operator she has used in her preparation and measurement match for a given qubit, they take it. Otherwise, they discard.
(4) *Authentication*: Alice and Bob announce publicly the result of part of the qubits that remain. If they are all the same, it means that no eavesdropper tried to intercept the communication,and therefore they can use the rest of the qubits as a key.
• Eavesdropping: If Eve tries to obtain the key, she will have to make measurements. Then, she will disturb the state, and the authentication will tell Alice and Bob of the presence of Eve. The important point here is that Eve does not know the operators selected by Alice and Bob until Bob performs the measurement and publicly announces it. For example, imagine that Alice prepares the qubit in the state $|1\rangle_x$. Consider the following two cases: (a) If Eve happens to measure σ_x, then she will measure 1 and will send again the state $|1\rangle_x$ to Bob; in that case, Alice and Bob cannot tell anything about the presence of Eve; (b) on the contrary, is she happens presence of σ_z then she will obtain 0 or 1 with probability 1/2. If she obtains 1, she will send the state $|1\rangle_z$ to Bob, which is not the one send by Alice. Therefore, in the process of authentication there is a probability 1/2 that Alice and Bob check that there is an error. Analogous conclusions applies if Eve measures 0. The probability for Eve to be detected if she measures every qubit using this procedure is $1 - (3/4)^N$ if Alice and Bob use N qubits in the authentication.

4.2.2 E91 Protocol

• Idea: ALice and Bob share pairs of two-level systems prepared in the singlet state:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) \tag{4.2}$$

The idea is that if they measure one of these pairs along the same direction (that is, measure the same $\sigma_{\vec{n}}$ they will obtain completely correlated results. That is, if one measures -1 the other will measure 1 and vice-versa. Thus, they can establish the key by simply taking -1 → 0 and by Alice exchanging 0 ↔ 1.
• Procedure:
(1) *Preparation and transmission*: A source emits pairs of two-level systems (qubits) in a singlet state. The particles fly apart towards the two legitimate users of the channel (Alice and Bob).
(2) *measurement*: Alice and Bob perform measurement of the spin components along three different directions given by unit vectors $\vec{a}_i$ for Alice and $\vec{b}_j$ for Bob $(i, j = 1, 2, 3)$. Both $\vec{a}_i$ and $\vec{b}_j$ vectors lie in the $x - y$ plane, and characterized by azimuthal angles $\phi_1^a = 0, \phi_2^a = \frac{\pi}{4}, \phi_3^a = \frac{\pi}{2}$ and $\phi_1^a = \frac{\pi}{4}, \phi_2^a = \frac{\pi}{2}, \phi_3^a = \frac{3\pi}{4}$. They use choose these orientations randomly and independently for each pair.
(3) *Public discussion*: Alice and Bob announce publicly the directions used in each measurement, and divide the measurements in two separate groups: a first group for which they used different orientations, and a second one for which they used the same.
(4) *Authentication*: Alice and Bob reveal publicly the results they obtained but within the first group only. With these measurements the check whether their measurements violate CHSH inequality (i.e. if the value of $S = 2\sqrt{2}$). In case they find $S = 2\sqrt{2}$ they used the results of the second group to establish the key.
• Eavesdropping: Any attempt of Eve to measure or modify the singlet states will disturb them, and therefore S will decrease (for the set of measurements described about $S = 2\sqrt{2}$ only for a singlet state; otherwise it is smaller).
• Similarities: The BB84 and E91 protocols for quantum public key distributions are similar. In fact, one see the E91 protocol as follows: if Alice measures along the z direction and obtains $|0\rangle_z$ ($|1\rangle_z$). If Alice measures along the x direction and obtains $|0\rangle_x$ ($|1\rangle_x$). Therefore, Alice can prepare the sequence of random states as in the BB84 form by performing appropriate measurements on singlet pairs.

4.2.3 B92 Protocol

• Two nonorthogonal states: There is a simple way to achieve quantum public key distribution using two nonorthogonal states $|u_0\rangle$ and $|u_1\rangle$. The idea is that since they are not orthogonal any eavesdropper sill change the state when trying to find out the state, since two nonorthogonal states cannot be distinguished.

• Procedure:
(1) *Preparation and transmission*: Alice prepares and sends Bob a random binary sequence of quantum system, using states $|u_0\rangle$ and $|u_1\rangle$ to present the bits 0 and 1.
(2) *measurement*: Bob decides, randomly and independently of Alice for each system, whether to subject it to a measurement $P_1 = 1 - |u_0\rangle \langle u_0|$ or $P_0 = 1 - |u_1\rangle \langle u_1|$. If Alice prepared $|u_0\rangle$ and Bob measured P_1, then the result will always be negative, whereas if Bob measured P_0 the result can be positive. Analogously if Alice prepared $|u_1\rangle$ and Bob measured P_0, then the result will always be negative, whereas if Bob measured P_1 the result can be positive.
(3) *Public discussion*: Bob publicly tells ALice in which instances his measurements had a positive result (but not which measurement he made), and the two parties agree to discard all the other instances. If there has been no eavesdropping, the remaining instances, a fraction approximately $(1 - |\langle u_0|u_1\rangle|^2)/2$ of the original trials should be perfectly correlated, consisting of instances in which Alice sent $|u_0\rangle$ ($|u_0\rangle$) and Bob measure P_0 (P_1).
(4) *Authentication*: Alice and Bob compare a sub-ensemble of the remaining instances to check for complete correlation.
• Eavesdropping: If Eve tried to measure the states sent by Alice, then she modifies the states, which will be revealed in the authentication step.

4.3 Teleportation

• Definition: By teleportation we define to transfer an intact quantum state from one place to another, by a sender who knows neither the state to be teleported nor the location of the intended received. The term teleportation comes from Science Fiction meaning to make a person of object disappear while an exact replica appears somewhere else.
Idea: Alice has a two-level system in an unknown state $|\phi\rangle$, and she wants to teleport it to Bob, whose location is not known. Prior to the teleportation process, Alice and Bob share an EPR pair. The idea is that Alice performs a joint measurement of the two-level system to be teleported and her EPR particle. Due to the nonlocal correlations, the effect of the measurement is that the unknown state appears instantaneously in Bob's hands, expect for s unitary operation which depends on the outcome of the measurement. If Alice communicate to Bob the result of her measurement, then Bob can perform that operation and therefore recover the unknown state.
• Initial states: let us call particle 1 that which has the unknown state $|\phi\rangle_1$, particle 2 the member of the EPR that Alice possesses and particle 3 that of Bob. We write the state of particle 1 as

$$|\phi\rangle_1 = a\,|0\rangle_1 + b\,|1\rangle_1 \tag{4.3}$$

where a and b are (unknown) complex coefficients. The state of particles 2 and 3 is the singlet state

$$|\Psi^-\rangle_{23} = \frac{1}{\sqrt{2}}(|0\rangle_2 |1\rangle_3 - |1\rangle_2 |0\rangle_3). \tag{4.4}$$

The complete state of particles 1, 2 and 3 is therefore

$$\begin{aligned} |\Psi\rangle_{123} =& \frac{a}{\sqrt{2}}(|0\rangle_1 |0\rangle_2 |1\rangle_3 - |0\rangle_1 |1\rangle_2 |0\rangle_3) \\ &+ \frac{b}{\sqrt{2}}(|1\rangle_1 |0\rangle_2 |1\rangle_3 - |1\rangle_1 |1\rangle_2 |0\rangle_3). \end{aligned} \tag{4.5}$$

Using the Bell basis for particles 1 and 2,

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}} (|0\rangle_1 |1\rangle_2 \pm |1\rangle_1 |0\rangle_2) \tag{4.6a}$$

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}} (|0\rangle_1 |0\rangle_2 \pm |1\rangle_1 |1\rangle_2) \tag{4.6b}$$

we find

$$\begin{aligned} |\Psi\rangle_{123} =& \frac{1}{2}\{|\Psi^-\rangle_{12} (-a |0\rangle_3 - b |1\rangle_3) \\ &+ |\Psi^+\rangle_{12} (-a |0\rangle_3 + b |1\rangle_3) \\ &+ |\Phi^-\rangle_{12} (a |0\rangle_3 + b |0\rangle_3) \\ &+ |\Phi^+\rangle_{12} (a |0\rangle_3 - b |0\rangle_3)\} \end{aligned} \tag{4.7}$$

• Procedure:
(1) *Alice measurement*: Alice makes a joint measurement of her particles (1 and 2) in the Bell Basis (4.6).
(2) *Alice broadcasting*: Then she broadcasts (classically) the outcome of her measurement.
(3) *Bob restoration*: Bob then applies a unitary operation to his particle to obtain $|\psi\rangle_3$. According to the state of the particles (4.7) the possible outcomes are:
- With probability 1/4, Alice founds $|\Psi^-\rangle_{12}$. The state of the third particle is automatically projected onto

$$-a |0\rangle_3 - b |1\rangle_3 . \tag{4.8}$$

Thus, in this case Bob does not have to perform any operator.
- With probability 1/4, Alice founds $|\Psi^+\rangle_{12}$. The state of the third particle is automatically projected onto

$$-a |0\rangle_3 + b |1\rangle_3 . \tag{4.9}$$

Teleportation occurs if Bob applies σ_z to his particle.

- With probability 1/4, Alice founds $|\Phi^-\rangle_{12}$. The state of the third particle is automatically projected onto

$$a\,|0\rangle_3 + b\,|1\rangle_3\,. \tag{4.10}$$

Teleportation occurs if Bob applies σ_x to his particle.
- With probability 1/4, Alice founds $|\Phi^+\rangle_{12}$. The state of the third particle is automatically projected onto

$$a\,|0\rangle_3 - b\,|1\rangle_3\,. \tag{4.11}$$

Teleportation occurs if Bob applies σ_y to his particle.
• Remarks: (1) Alice ends up with no information of her original state. In this sense, the state of particle 1 has been swapped to particle 3.
(2) There is no instantaneous propagation of information. Bob has to wait until he receives the (classical) message from Alice with her outcome. Before he receives the message, his lack of knowledge prevents him from having the state. Note that no measurement can tell him whether Alice has performed her measurement or not.
(3) Since teleportation is a operation applied to a state, it will also work for statistical mixtures, or in the case in which particle 1 in entangled with other particles. This might be interesting in the sense that it might allow teleportation between any two partners of a network, each of them shares singlet states with a center.
(4) One can also generalize teleportation to N-level systems.

4.4 Dense Coding

• Idea: Given a maximally entangled state, one can prepare ant other maximally entangled state using local operations. In particular, one can prepare all four elements of the Bell basis. Thus if Alice sends the member of an EPR pair to Bob, he can apply one of the four unitary operations and obtain 4 orthogonal states of the particles. Then, sending the particle back to Alice, she can know the operation performed by Bob. In this case, Bob can send two bits of information by only acting on one particle.
• Procedure: Alice has two particles in a singlet state $|\Psi^-\rangle_{AB}$. Then sends one to Bob, who applies a local operation (i.e. a unitary operator on particle 2). This operation can be written in terms of the Euler angles

$$U_B = U_B(\alpha,\beta,\gamma) = e^{-i\alpha\sigma_x^B}\,e^{-i\beta\sigma_y^B}\,e^{-i\gamma\sigma_z^B} \tag{4.12}$$

Then we obtain Thus, Bob can produce all the states of the form

$$|\psi_{\alpha,\beta,\gamma}\rangle_{AB} = U\,|\Psi^-\rangle_{AB} \tag{4.13}$$

In particular, we have that,except for irrelevant phase factors,

$$|\psi(0,0,0)\rangle_{AB} = |\Psi^-\rangle_{AB} \,, \tag{4.14a}$$

$$|\psi(0,0,\pi/2)\rangle_{AB} = |\Psi^+\rangle_{AB} \,, \tag{4.14b}$$

$$|\psi(0,\pi/2,0)\rangle_{AB} = |\Phi^-\rangle_{AB} \,, \tag{4.14c}$$

$$|\psi(\pi/2,\pi/2,0)\rangle_{AB} = |\Phi^+\rangle_{AB} \,, \tag{4.14d}$$

Thus, by choosing different Euler angles, Bob can prepare any of the state of Bell's basis. Since these states are orthogonal, he can encode 2 bits in his action. Then he sends back the particle, and Alice measures in the Bell basis.

4.5 Classical Computing

• Computation: A computation can be considered as a physical process that transforms an *input* into an *output.* A classical computation is that in which the physical process is based on classical laws (without coherent quantum phenomena).
• Slow and Fast Algorithms: Algorithms to compute operations can be classified in terms of the relationship between the member of steps required n_s and the size of the input (number of bits; the size of a number N in $\log_2(N)$):
(1) *Fast*: The number of steps scale as a polynomial of the size of the input, that is $n_s \leq \text{poly}[\log_2(N)]$ for all N.
(2) *Slow*: The number of steps scale cannot be bounded by a given polynomial of the size of the input, that is $n_s > \text{poly}[\log_2(N)]$ for any given polynomial and certain N.
• Example: Multiplication by the number 123 requires $n_s < k\log_2(N)$ (for a given k), and therefore is fast. The factorization of a number using an algorithm that checks if it is a divisor of 1, 2, ..., $\sqrt{N}$ requires $\sqrt{N} = 2^{\log_2(N)/2}$, and therefore it is slow.
• Universal Computers: One would like to have computers that are able to perform any algorithm; that is, changing from one algorithm to another should be done by the software. This leads to the concept of bits and gates.
(1) Bits: Bits are (classical) systems with two different states 0 and 1. Any input and output number can be encoded in these system using binary notation. For example, is we have 5 bits we can represent the number 23 as 10111.
(2) Gates: The gates are processes that transform bits. For examples,

NOT	
Input	Output
0	1
1	0

AND		
Input		Output
0	0	0
0	1	0
1	0	0
1	1	1

(3) Universal Gates: These are a finite set of gates (AND, NOT, ...) such that any computation can be performed by a sequence of these gates.
• Quantum Computation: A *quantum computation* can be considered as a physical process that transforms an *input* state into an *output* state of a system. The physical process is based on coherent quantum phenomena.
(1) Inputs and Outputs: Inputs and outputs are represented by states of the system. For example, enumerating the state of a given basis as $|1\rangle, |2\rangle, ...$,the number N would be represented by the N-th state of this basis.
(2) Restrictions: The operation that transforms input into outputs has to be unitary. For example, the operation that given 1 if a number is odd and 2 it is even could not be implemented:

$$|1\rangle \to |1\rangle, |2\rangle \to |2\rangle, |3\rangle \to |1\rangle, |4\rangle \to |2\rangle .$$

This operation cannot be unitary since it is not reversible. One can however use an auxiliary system so that the output is written in that system:

$$|1\rangle |0\rangle \to |1\rangle |1\rangle, |2\rangle |0\rangle \to |2\rangle |2\rangle, |3\rangle |0\rangle \to |3\rangle |1\rangle, |4\rangle |0\rangle \to |4\rangle |2\rangle .$$

(3) Quantum Parallelism: Using the laws of Quantum Mechanics, one can do more than with the laws of Classical Mechanics. To compute a function $f : N \to N$ for the numbers 1,2,..,n, classically one has to run the computer n times. In a quantum computer one can do the same:

$$|1\rangle |0\rangle \to |1\rangle |f(1)\rangle, \; |2\rangle |0\rangle \to |2\rangle |f(2)\rangle, ... |n\rangle |0\rangle \to |n\rangle |f(n)\rangle .$$

Alternatively, one can prepare an input state that is a superposition

$$|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} |k\rangle |0\rangle , \tag{4.15}$$

and run the computer on this stay only, obtaining

$$\frac{1}{\sqrt{n}} \sum_{k=1}^{n} |k\rangle |f(k)\rangle . \tag{4.16}$$

All the values of f are in this superposition. However, it is not possible to read them out in a measurement.
(4) Conditional Dynamics: Some operations can be viewed as conditional dynamics, that is, the second system evolves depending on the state of the first system. For example, one can have

$$U = |1\rangle \langle 1| U_1 + |2\rangle \langle 2| U_2 + ... \tag{4.17}$$

where U_i is a unitary operator acting on the second system.
• Slow and Fast Algorithms: All operations that have fast algorithms in classical computation have fast algorithms in quantum computation. However, there are operations for which only classical slow algorithms exists, but there are quantum

fast algorithms. The most important example is factorization.
• Deutsch-Jozsa Algorithm: Consider the following problem. Consider the four operations f_1, f_2, g_1, g_2 acting on the numbers $x = 0, 1$: f_1 =I (I=identity), f_2= NOT, $g_1 = (1-x) \cdot I + x\cdot$NOT, and $g_2 = x \cdot I + (1-x)\cdot$NOT. That is, the first two (f_1, f_2) give different results if acting on 0,1, whereas the second two $(g_1.g_2)$ given the same result. Somebody give us one function h and we have to check whether it belongs to the first group or to the second. The application of the function takes 13 hours every time, and we have to give the result in less than 24 hours.
(1) Classically: Classically, we have to prepare an input state $|n_1\rangle \otimes |n_2\rangle$. The output state will be $|n_1\rangle \otimes |f(n_1)\rangle$. We prepare the input state

$$|\psi_{in}\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle). \tag{4.18}$$

The corresponding outputs for each possible functions are:

$$f_1 |\psi\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle), \tag{4.19a}$$

$$f_2 |\psi\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (-|0\rangle + |1\rangle), \tag{4.19b}$$

$$f_3 |\psi\rangle = \frac{1}{2}(|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle), \tag{4.19c}$$

$$f_4 |\psi\rangle = \frac{1}{2}(|0\rangle - |1\rangle) \otimes (-|0\rangle + |1\rangle). \tag{4.19d}$$

The result given by f_1 and f_2 are orthogonal to those given by g_1 and g_2, and therefore we can distinguish whether we applied one of the f or g functions (for example, measuring σ_x in the first system).
• Universal Quantum Computers: As in the classical case, one would like to have quantum computers that are able to perform any algorithm; that is, changing from one algorithm to another should be done by the software. This leads to the concept of qubits and quantum gates.
(1) Qubits: Qubits are (quantum) systems with two different state $|0\rangle$ and $|1\rangle$. Any input and output number can be encoded in these systems using binary notation. For example, if we have 5 qubits we can represent the number $|23\rangle$ as $|10111\rangle$.
(2) Quantum Gates: These are quantum processes and transform qubits. For example,

Single qubit gate: I(α,ϕ)

Input	Output
$\lvert 0\rangle$	$\cos(\alpha)\lvert 0\rangle - ie^{i\phi}\sin(\alpha)\lvert 1\rangle$
$\lvert 1\rangle$	$-ie^{i\phi}sin(\alpha)\lvert 0\rangle + \sin(\alpha)\lvert 0\rangle$

2-qubit gate: Control-NOT

Input		Output	
$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$
$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$
$\lvert 1\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 1\rangle$
$\lvert 1\rangle$	$\lvert 1\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$

(3) Universal Gates: It can be shown that any unitary operation acting on a set of qubits can be written as a sequence of Control- NOT and single qubit gates.

4.6 The Introduction of Quantum Identification

• Goal: We wish to design a scheme in which two partners (Alice and Bob) can identify one each other (or, at least, one of them can identify the other one). The scheme has to be secure against Eve, who may try to impersonate either Alice or Bob.
• Classical: Consider first a simple classical identification scheme: Bob has a *code* (sequence of zeros and ones) and Alice knows this sequence. By reading the sequence she can determine whether a given code in correct or not. This scheme is partially secure against Eve. On the one hand, by choosing a random sequence of zeros and ones she can impersonate Bob with a probability $P = 1/2^N$, where N is the length of the code. For N large, this probability can be arbitrarily small. On the other hand, however, if Eve has access to Bob's code she can copy it an impersonate him.
• Quantum: Here we will give three alternative identification schemes based on quantum mechanics principles, that are most secure than the classical one. Each of these procedures have their own advantages, and are designed for different situations.

4.7 Random Polarization Scheme

4.7.1 Procedure

• Goal: This first scheme allows Alice to identify Bob.
• States: Bob has a set of N two-level systems $b_1, b_2, ..., b_N$ polarized along different directions, namely

$$|\Psi\rangle_{b_k} = \cos(\theta_k/2)\,|0\rangle_{b_k} + \sin(\theta_k/2)e^{i\phi_k}\,|1\rangle_{b_k}\,, \tag{4.20}$$

is the state of the k-th particle, where θ_k and ϕ_k define the polarization direction.
• Identification: If Alice knows these directions (i.e., all these angles), she can identify Bob with probability one by simply performing measurements along the corresponding directions.

4.7.2 Security

• Strategy 1: Suppose Eve prepares a state like (4.20) but with random coefficients. In the basis in which the which the state $|\Psi\rangle_{e_k} = |0\rangle$, we can write

$$|\Psi\rangle_{e_k} = \cos(\theta_r/2)\,|0\rangle_{e_k} + \sin(\theta_r/2)e^{i\phi_r}\,|1\rangle_{e_k}\,, \tag{4.21}$$

where now θ_r and ϕ_r are random coefficients. The probability for Alice to measure the state $|\Psi\rangle_{e_k}$ and obtain $|0\rangle$ (i.e., a positive identification) is $P_k = \cos^2(\theta_r/2)$. Averaging over the random variable θ_r, this probability is $P_k = 1/2$. For N particles the probability for Eve to impersonate Bob is then $P_E = 1/2^N$.
• Strategy 2: Suppose now that Eve measures Bob's particles in a given basis defined by

$$|\widetilde{0}\rangle_{e_k} = \cos(\theta_r/2)\,|0\rangle_{e_k} + \sin(\theta_r/2)e^{i\phi_r}\,|1\rangle_{e_k}\,, \tag{4.22a}$$

$$|\widetilde{1}\rangle_{e_k} = \sin(\theta_r/2)\,|0\rangle_{e_k} - \cos(\theta_r/2)e^{i\phi_r}\,|1\rangle_{e_k}\,. \tag{4.22b}$$

Depending on the result, she prepares her particle e_k in $|0\rangle_{e_k}$ or $|1\rangle_{e_k}$. Then she tries to impersonate Bob with these particles. The probability for a positive identification with the k-th particles is $p_k = |\langle 0|\widetilde{0}\rangle|^2 + |\langle 0|\widetilde{1}\rangle|^2 = 1 - 2\cos^2(\theta_r/2)\sin^2(\theta_r/2)$. Averaging over the angle θ_r we get $P_k = 2/3$. For N particles, the probability to impersonate Bob is then $P_E = (2/3)^N$.
• Many Particles: Finally, using the results of Massar and Popescu [Phys. Rev. Lett. **74**, 1259 (1995)] one can easily show that using the best measurement strategy (using ancilla, etc), if then are X copies of the state of each particle $|\Psi\rangle_{b_k}$, Eve can impersonate Bob with a probability $P \leq |X+1)(X+2)|^N$. For $X, N \gg 1, P \rightarrow e^{-N/X}$.

4.7.3 Properties

• As in the classical case, the probability for Eve to impersonate Bob by choosing a set of N two-level systems polarized along random directions is $P_E = 1/2^N$.
• As opposed to the classical scheme.Eve cannot copy Bob's code unless she knows the directions along which the particles are polarized. By measuring Bob's particles she can prepare a code that allows her to impersonate Bob with probability $P_E = (2/3)^N$.
• Alice could prepare a set of N identical codes and give them not only to Bob but also to other people (this would be like a VIP card). However, in that case Eve could perform measurements that would allow her to guess Bob's code with a probability $P_E \approx e^{-N/X}$. Thus, to keep the scheme secure it is required that $X \ll N$.
• There must be somebody (ALice) who knows the code in order to perform the identification. This might be dangerous since she can also given the code to Eve.

4.8 Non-Orthogonal States Scheme

4.8.1 Procedure

• Goal: This second scheme allows Alice and Bob to identify one each other.
• States: Both Alice and Bob have a set of N particles. We will denote Alice and Bob's particles by $a_1, a_2, ..., a_N$ and $b_1, b_2, ..., b_N$, respectively. Each pair (a_i, b_i) is prepared in the same state, either $|\widetilde{0}\rangle$ or $|\widetilde{1}\rangle$, that are defined according to

$$|\widetilde{0}\rangle = |0\rangle\,, \tag{4.23a}$$

$$|\widetilde{1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{4.23b}$$

where $|0\rangle$ and $|1\rangle$ are two orthogonal states.
• Identification: In order to carry out the identification procedure, Alice and Bob compare the state of each pair (a_i, b_i). If all the states in each pair coincide, the identification is positive. For the comparison between a_i and b_i one uses an ancilla x_i, initially in the state $|0\rangle_{x_i}$, and performs the (unitary) transformation T

$$|\widetilde{0}\rangle_{a_i} |\widetilde{0}\rangle_{b_i} |0\rangle_{x_i} \to |\widetilde{0}\rangle_{a_i} |\widetilde{0}\rangle_{b_i} |1\rangle_{x_i}\,, \tag{4.24a}$$

$$|\widetilde{1}\rangle_{a_i} |\widetilde{1}\rangle_{b_i} |0\rangle_{x_i} \to |\widetilde{1}\rangle_{a_i} |\widetilde{1}\rangle_{b_i} |1\rangle_{x_i}\,. \tag{4.24b}$$

Then, the state of all the ancilla is detected. If all them are in $|1\rangle$, this gives a positive result.
• Details if the Scheme: We define the following basis in the subspace corresponding to the product space of particles a_i and b_i:

$$|A\rangle = |0\rangle_{a_i} |0\rangle_{b_i}\,, \tag{4.25a}$$

$$|B\rangle = \frac{1}{\sqrt{3}}(|1\rangle_{a_i} |1\rangle_{b_i} + |0\rangle_{a_i} |1\rangle_{b_i} + |1\rangle_{a_i} |0\rangle_{b_i}), \tag{4.25b}$$

$$|C\rangle = \frac{1}{\sqrt{6}}(2\,|1\rangle_{a_i} |1\rangle_{b_i} - |0\rangle_{a_i} |1\rangle_{b_i} - |1\rangle_{a_i} |0\rangle_{b_i}), \tag{4.25c}$$

$$|D\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{a_i} |1\rangle_{b_i} - |1\rangle_{a_i} |0\rangle_{b_i}). \tag{4.25d}$$

Using the relations:

$$\begin{aligned}
|\widetilde{0}\rangle_{a_i} |\widetilde{0}\rangle_{b_i} &= |A\rangle\,, \\
|\widetilde{1}\rangle_{a_i} |\widetilde{1}\rangle_{b_i} &= \frac{1}{2}(|A\rangle + \sqrt{3}\,|B\rangle), \\
|\widetilde{0}\rangle_{a_i} |\widetilde{1}\rangle_{b_i} &= \frac{1}{2\sqrt{3}}(\sqrt{6}\,|A\rangle + \sqrt{2}\,|B\rangle - |C\rangle + \sqrt{3}\,|D\rangle), \\
|\widetilde{1}\rangle_{a_i} |\widetilde{0}\rangle_{b_i} &= \frac{1}{2\sqrt{3}}(\sqrt{6}\,|A\rangle + \sqrt{2}\,|B\rangle - |C\rangle - \sqrt{3}\,|D\rangle),
\end{aligned}$$

it is readily shown that the unitary transformation defined by

$$|A\rangle\,|0\rangle_{x_i} \to |A\rangle\,|1\rangle_{x_i} \tag{4.26a}$$

$$|B\rangle\,|0\rangle_{x_i} \to |B\rangle\,|1\rangle_{x_i} \tag{4.26b}$$

$$|C\rangle\,|0\rangle_{x_i} \to |C\rangle\,|0\rangle_{x_i} \tag{4.26c}$$

$$|D\rangle\,|0\rangle_{x_i} \to |D\rangle\,|0\rangle_{x_i} \tag{4.26d}$$

implements (4.24). Besides, we have

$$\begin{aligned} |\widetilde{0}\rangle_{a_i}\,|\widetilde{1}\rangle_{b_i}\,|0\rangle_{x_i} \to & \frac{1}{2\sqrt{3}}\{(\sqrt{6}\,|A\rangle + \sqrt{2}\,|B\rangle)\,|1\rangle_{x_i} \\ & - (|C\rangle - \sqrt{3}\,|D\rangle)\,|0\rangle_{x_i}\} \end{aligned} \tag{4.27a}$$

$$\begin{aligned} |\widetilde{1}\rangle_{a_i}\,|\widetilde{0}\rangle_{b_i}\,|0\rangle_{x_i} \to & \frac{1}{2\sqrt{3}}\{(\sqrt{6}\,|A\rangle + \sqrt{2}\,|B\rangle)\,|1\rangle_{x_i} \\ & - (|C\rangle + \sqrt{3}\,|D\rangle)\,|0\rangle_{x_i}\} \end{aligned} \tag{4.27b}$$

4.8.2 Security

• Strategy 1: Suppose that Eve prepares her k-th particle in a random state(with equal probability distribution) $|\widetilde{0}\rangle_{e_k}$ or $|\widetilde{1}\rangle_{e_k}$. The probability for Alice to measure Eve's particle in the same state as Bob's is, according to (4.24) and (4.27), $P_k = 5/6$. Therefore, $P_E = (5/6)^N$.
• Strategy 2: On the other hand, if Eve can measure the state of Bob's particle, she can find a better strategy to try to impersonate Bob. For example, she can choose $|\widetilde{0}\rangle_{e_k}$ or $|\widetilde{1}\rangle_{e_k}$ when she measures $|\widetilde{0}\rangle_{e_k}$ or $|\widetilde{1}\rangle_{e_k}$, respectively. Using again (4.24) and (4.27) one can show that the probability in this case to impersonate Bob is $P_E = (11/12)^N$.

4.8.3 Properties

• Alice and Bob do not need to know the code. In face, the code can be completely random and unknown. In this sense, this code is more secure than the previous one.
• The probability for Eve to impersonate Bob by choosing a set of N two-level systems prepared in random states $|\widetilde{0}\rangle_{e_k}$ or $|\widetilde{1}\rangle_{e_k}$ is $P_E = (5/6)^N$.
• Eve cannot copy Bob's cede. What she can do is to measure Bob's particles and prepare a sequence according to the measurements. In this case, one also gets an exponential decreasing of the probability with N, namely $P_E = (11/12)^N$.
• As before, there can be $X \geq 1$ codes,and identification can take place among the corresponding partners. Again, it is required $N \gg X$ in order for the code to remain secure.

4.9 Entanglement Scheme

4.9.1 Procedure

• Goal: This scheme, as the previous one, allows Alice and Bob to identify one each other.
• States: Alice and Bob have to both a set of N particles. Now, each of the pairs (a_i, b_i) is in an entangle state. More specifically, the state of Alice and Bob's particles is

$$|\Psi\rangle_{A,B} = \prod_{i=1}^{N} |\psi^+\rangle_{a_i,b_i}, \tag{4.28}$$

where $|\psi^+\rangle$ denotes one of the Bell basis states

$$|\varphi^\pm\rangle_{a,b} = \frac{1}{\sqrt{2}}(|0\rangle_a |0\rangle_b \pm |1\rangle_a |1\rangle_b), \tag{4.29a}$$

$$|\phi^\pm\rangle_{a,b} = \frac{1}{\sqrt{2}}(|0\rangle_a |1\rangle_b \pm |1\rangle_a |0\rangle_b). \tag{4.29b}$$

• Identification: The procedure consists of detecting whether each pair (a_i, b_i) is in the state $|\phi^\pm\rangle$. For example, one could perform the measurements in the basis (4.29), If all pairs are detected in the state $|\phi^+\rangle$, the identification is positive.

4.9.2 Security

• Strategy 1: Let us consider that Eve has N particles, $e_1, e_2, ..., e_n$ in states

$$|\eta^i\rangle_{e_i} = \alpha_i |0\rangle_{e_i} + \beta_i |1\rangle_{e_i}, \tag{4.30}$$

where α_i, β_i are two complex with $|\alpha|^2 + |\beta|^2 = 1$. She uses these particles to try to supplant either ALice or Bob. Let us calculate the probability of success. Using that

$$|\varphi^+\rangle_{a_i,b_i} |\eta^i\rangle_{c_i} = \frac{1}{2} |\eta^i\rangle_{a_i} |\varphi^+\rangle_{b_i,c_i} + \frac{\sqrt{3}}{2} |\Psi_i^\perp\rangle_{a_i,,b_i,c_i}, \tag{4.31}$$

where the two states in the rhs of this equation are orthogonal, we can write

$$\begin{aligned} |\Psi\rangle_{A,B,E} &\equiv \prod_{i=1}^{N} |\varphi^+\rangle_{a_i,b_i} |\eta^i\rangle_{e_i} \\ &= \frac{1}{2^N} |\Psi_P\rangle_{A,B,E} + \frac{1}{[1-2^{2N}]^{1/2}} |\Psi_P^\perp\rangle_{A,B,E}, \end{aligned} \tag{4.32}$$

where

$$|\Psi_P\rangle_{A,B,E} = \prod_{i=1}^{N} |\eta^i\rangle_{a_i} |\varphi^+\rangle_{b_i,e_i} \tag{4.33}$$

and $\langle\Psi_P|\Psi_P^{\perp}\rangle = 0$. The probability for Eve to impersonate Bob is $P_E = |\langle\Psi_P|\Psi_P\rangle|^2 = 1/2^{2N}$. Note that this result is independent of the states $|\eta^i\rangle$. Obviously, the same result is obtained if Eve tries to impersonate Bob.

• Strategy 2: Suppose that Eve measures the state of Alice's particles and then tries to impersonate her with a set of particles $e_1, e_2, ..., e_N$ as before. For example, if Eve measures Alice's i-th particle in state $|0\rangle$, the state $|\varphi^+\rangle_{a_i,b_i}$ is projected onto $|0\rangle_{a_i}|0\rangle_{b_i}$. Since we can write

$$|0\rangle_{a_i}|0\rangle_{b_i} = \frac{\alpha_i}{\sqrt{2}}|0\rangle_{\alpha_i}|\varphi^+\rangle_{b_i,e_i} + \frac{1}{[1-|\alpha_i|^2/2]^{1/2}}|\Psi_i^{\perp}\rangle_{a_i,b_i,e_i}\,, \tag{4.34}$$

the probability of finding the pair (b_i, c_i) in the state $|\varphi^+\rangle$ is $|\alpha|^2/2 \leq 1/2$. In a similar way, if Eve measures Alice's i-th particle in state $|1\rangle$, the probability of finding the pair (b_i, c_i) in the state $|\varphi^+\rangle$ is $|\beta|^2/2 \leq 1/2$. In consequence, $P_k \leq 1/2$. Thus, the probability of impersonating Bob is always $P_E \leq 1/2^N$.

• Subsequent Trials: SInce after a positive identification between Alice and Bob's state of their identifications. We will show that of somebody tries to impersonate either of them obtaining a negative result. Alice and Bob codes are still useful for identification. For this to be true it is needed that Alice and Bob's measurement projects either onto the subspace corresponding to all the pairs in state $|\varphi\rangle$, or onto the orthogonal one.

Let us assume that Eve tries to impersonate X times either Alice or Bob using N particles (in each trial). Let us denote by $|\eta_{i,j}\rangle_{e_i}$, $(i = 1, 2, ..., N, j = 1, 2, ..., X)$ the state of the i-th particle at the j-th trial. The state of all particles (including Alice and Bob's) will be

$$|\Psi\rangle \equiv \prod_{i=1}^{N}|\varphi^+\rangle_{a_i,b_i}\prod_{j=1}^{X}|\eta_{i,j}\rangle_{e_{i,j}} = \frac{1}{2^N}\sum_{j=1}^{X}|\Phi_k\rangle + \kappa|\Psi^{\perp}\rangle, \tag{4.35}$$

where

$$|\Phi_k\rangle = \prod_{i=1}^{N}\{\prod_{j\neq k}^{X}|\eta_{i,j}\rangle_{e_{i,j}}\}|\eta_{i,k}\rangle_{a_i}|\varphi^+\rangle_{b_i,e_{i,k}} \tag{4.36}$$

and $\kappa < 1$ is a normalization constant. Using Eqs. (4.35) and (4.31) and it can be shown that

$$|\langle\Phi_k|\Phi_{k'}\rangle| = \frac{1}{2^N}\prod_{i=1}^{N}|\langle\eta_{i,k}|\eta_{i,k'}\rangle|^2 \leq \frac{1}{2^N}, \tag{4.37a}$$

$$|\langle\Phi_k|\Phi\rangle| = 1/2^N \tag{4.37b}$$

respectively. Thus,

$$\kappa^2 = ||\,|\Psi\rangle - \frac{1}{2^N}\sum_{k=1}X|\Phi_k\rangle||^2 = 1 - \frac{X}{2^{2N}} + \frac{X}{2^{2N}} \tag{4.38}$$

Furthermore, using (4.37b) we have

$$|\langle\Phi_k|\Psi^{\perp}\rangle| \leq \frac{X}{2^{2N}}. \tag{4.39}$$

Now we calculate the probability of a positive result for Eve in at least one of the X trials. This probability is given by

$$P_E^X = \sum_{k=1}^{X} |\left\langle \Phi_k | \Psi \right\rangle|^2 = \frac{X}{2^{2N}}, \tag{4.40}$$

where we have used (4.40).
Finally, the probability that after X unsuccessful trials, Alice and Bob identify each other is

$$P_E^X = |\left\langle \Phi_k | \Psi^{\perp} \right\rangle|^2 = 1 - \frac{X}{2^{2N}} + \frac{X}{2^{2N}} \tag{4.41}$$

4.9.3 Properties

• There is no code. Thus, Eve cannot copy it or even guess it.
• The probability for Eve to impersonate Bob by choosing a set of N two-level systems is $P_E = 1/2^{2N}$. This is a factor $1/2^N$ smaller than in the classical state.
• If Eve measures the state of Bob's particles. the probability of impersonating Bob is still $P_E \leq 1/2^N$.
• There can only be two partners in the identification. Note, however, that for X partners one can prepare particles $(a_i, b_i, c_i ...)$ in an entangled state $\frac{1}{\sqrt{2}}(|000...\rangle + |111...\rangle)$. In this case, there can be a collective identification if all the partners are present.
• After a positive identification, the state $|\Psi\rangle_{A,B}$ is not changed, and therefore can be used for the future identifications.
• If one performs the measurements appropriately, the state after a negative identification (after an unsuccessful trial by Eve) is "almost" not perturbed. By this we mean that after X trials: (1) the probability for Eve to impersonate either Alice or Bob in a further trial is $P_E = X/2^{2N}$, (2) the probability for Bob to obtain a positive identification is still $1 - X/2^{2N}$.

Chapter 5

STATE PURIFICATION

5.1 Introduction

• Idea: We have seen that some of the applications of quantum coherent phenomena one needs ”perfect” (pure) entangled states of two distant systems. In realistic situations, nothing is perfect, so that the states will be mixed. In principle, these mixed states will not be good enough to carry out a teleportation process, or to perform quantum cryptography with them. The ideas is that if we have many pairs is mixed states, we may distill few pairs in almost pure states using only local operations.

5.2 Purification Using Local POVMS

• States: Imagine we have a large number of imperfect EPR pairs in the state

$$\rho = (1-x)\left|\Psi^-\right\rangle\left\langle\Psi^-\right| + x\left|11\right\rangle\left\langle 11\right|, \tag{5.1}$$

where $x \in [0,1)$. One of the members of each pair is in A and the other in B.
• CHSH Inequalities: Let us calculate if the state (5.1) violates CHSH inequalities. For this, we have to check whether

$$S \equiv |E(\vec{a},\vec{b}) - E(\vec{a},\vec{c})| + |E(\vec{b},\vec{d}) + E(\vec{d},\vec{c})| \tag{5.2}$$

is larger than 2. For the state (5.1), we can write

$$S = (1-x)S_{\Psi^-} + xS_{11} \tag{5.3}$$

where S_{Ψ^-} is (5.2) calculated with the single state, and S_{11} with the state $|11\rangle$. According to what we saw chapter 2. if we choose the vectors $\vec{a},\vec{b},\vec{c},\vec{d}$ is a plane, with the angles $\angle\vec{a},\vec{b} = \angle\vec{b},\vec{d} = \angle\vec{d},\vec{c} = \pi/4$, we have $S_{\Psi^-} = 2\sqrt{2}$. On the other hand, for the same angles we have $S_{11} = \sqrt{2}$. Therefore $S = 2\sqrt{2} - x\sqrt{2}$. For

$0 \leq x < 2 - \sqrt{2}$, CHSH inequalities are violated.
• Measurement: We measure the POVMs

$$A_1 = \alpha \left|0\right\rangle \left\langle 0\right| + \beta \left|1\right\rangle \left\langle 1\right|, \quad A_2 = \beta \left|0\right\rangle \left\langle 0\right| + \alpha \left|1\right\rangle \left\langle 1\right|, \tag{5.4}$$

with $\beta = 1 - \alpha \in (0, 1)$, both in A and B, for each of the pairs. If we obtain a positive result for A_1 in both sites, we keep the particles. Otherwise, we discard the particles.
• State After The Measurement: In a successful measurement, the state of the particles will be

$$\begin{aligned} \rho_s &= \frac{A_1^A A_1^B \rho A_1^B A_1^B}{Tr(A_1^A A_1^B \rho A_1^B A_1^B)} \\ &= \frac{1}{(1-x)\alpha^2 + x\beta^1} \\ &\times [(1-x)\alpha^2 \left|\Psi^-\right\rangle \left\langle \Psi^-\right| + x\beta^1 \left|11\right\rangle \left\langle 11\right|]. \end{aligned} \tag{5.5}$$

Thus, for $\alpha \to 1$, the state after a successful measurement will be as closed to the singlet state as we will.
• Probability Of Success: The probability of success is

$$Tr(A_1^A A_1^B \rho A_1^B A_1^B) = \beta^2[(1-x)\alpha^1 + x\beta^2], \tag{5.6}$$

i.e. tends to zero for $\alpha \to 1$.

5.3 Purification Using Local Controlled-NOT Operations

• Initial State: Imagine we have many distant pairs in A and B whose initial state ρ is such that the fidelity $F = \left\langle \Psi^-\right| \rho \left|\Psi^-\right\rangle > 1/2$ (that is, it is ”mostly” a singlet state). The goal of the purification is to perform local operations among the pairs to produce few pairs of larger fidelity.
• Procedure: (1) Random Bilateral Rotations: The observers in A and B apply random bilateral rotations to each pair. That is, they apply the same random unitary operation to the particles of each pair. The singlet state is $\left|\Psi^-\right\rangle$ is invariant under these rotations, whereas the orthogonal subspace is completely messed up (depolarized). Thus, the state after these rotations will be,

$$\begin{aligned} \rho_{\Psi} =& F \left|\Psi^-\right\rangle \left\langle \Psi^-\right| + \frac{1-F}{3} \left|\Psi^+\right\rangle \left\langle \Psi^+\right| \\ &+ \frac{1-F}{3} \left|\Phi^-\right\rangle \left\langle \Phi^-\right| + \frac{1-F}{3} \left|\Phi^+\right\rangle \left\langle \Phi^+\right|, \end{aligned} \tag{5.7}$$

where $\left|\Psi^+\right\rangle$ and $\left|\Phi^\pm\right\rangle$ are the other states of the Bell basis, which span the space orthogonal to the singlet state. Note that in this way one can always produce states of the form (5.7). These states are called Werner State.

(2) Unilateral Pauli Rotation: One of the observers performs the unitary transformation σ_y to his particles. This transforms $\Psi^{pm} \leftrightarrow \Phi^{\mp}$. The state after this rotation will be

$$\begin{aligned}\rho_{\Phi^+} =& F\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \frac{1-F}{3}\left|\Phi^-\right\rangle\left\langle\Phi^-\right| \\ &+ \frac{1-F}{3}\left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \frac{1-F}{3}\left|\Psi^-\right\rangle\left\langle\Psi^-\right|.\end{aligned} \tag{5.8}$$

The state (5.7) that had the maximum contribution coming from $\left|\Psi^-\right\rangle$ becomes now one with maximum contribution of Φ^+.
(3)Bilateral Controlled-NOT Operation: The observers take two pairs, and apply locally a controlled not operation to their two particles. Let us denote by A_1 and A_2 the particles in A and B_1 and B_2 the particles in B (the joint state of particles A_1 and B_1 is (5.8), the same as for particles A_2 and B_2)

$$\rho = \rho_{\Phi^+}^{A_1B_1}\rho_{\Phi^+}^{A_2B_2}. \tag{5.9}$$

We will call the particles 1 (A_1 and B_1) sources, and the other two (A_2 and B_2) target. The control-NOT operation acts as follows:

$$\left|0\right\rangle_{A_1}\left|0\right\rangle_{A_2} \to \left|0_{A_1}\right\rangle\left|0_{A_2}\right\rangle, \tag{5.10a}$$

$$\left|0\right\rangle_{A_1}\left|1\right\rangle_{A_2} \to \left|0_{A_1}\right\rangle\left|1_{A_2}\right\rangle, \tag{5.10b}$$

$$\left|1\right\rangle_{A_1}\left|0\right\rangle_{A_2} \to \left|1_{A_1}\right\rangle\left|1_{A_2}\right\rangle, \tag{5.10c}$$

$$\left|1\right\rangle_{A_1}\left|1\right\rangle_{A_2} \to \left|1_{A_1}\right\rangle\left|0_{A_2}\right\rangle, \tag{5.10d}$$

and similarly with B. The state of the particles after this operation can be derived using the following table:

Initial state		Final state	
Sources	Targets	Sources	Targets
$\left\|\Phi^\pm\right\rangle$	$\left\|\Phi^+\right\rangle$	$\left\|\Phi^\pm\right\rangle$	$\left\|\Phi^+\right\rangle$
$\left\|\Phi^\pm\right\rangle$	$\left\|\Phi^-\right\rangle$	$\left\|\Phi^\mp\right\rangle$	$\left\|\Phi^-\right\rangle$
$\left\|\Psi^\pm\right\rangle$	$\left\|\Psi^+\right\rangle$	$\left\|\Psi^\pm\right\rangle$	$\left\|\Phi^+\right\rangle$
$\left\|\Psi^\pm\right\rangle$	$\left\|\Psi^-\right\rangle$	$\left\|\Psi^\mp\right\rangle$	$\left\|\Phi^-\right\rangle$
$\left\|\Phi^\pm\right\rangle$	$\left\|\Psi^+\right\rangle$	$\left\|\Phi^\pm\right\rangle$	$\left\|\Psi^+\right\rangle$
$\left\|\Phi^\pm\right\rangle$	$\left\|\Psi^-\right\rangle$	$\left\|\Phi^\mp\right\rangle$	$\left\|\Psi^-\right\rangle$
$\left\|\Psi^\pm\right\rangle$	$\left\|\Phi^+\right\rangle$	$\left\|\Psi^\pm\right\rangle$	$\left\|\Psi^+\right\rangle$
$\left\|\Psi^\pm\right\rangle$	$\left\|\Phi^-\right\rangle$	$\left\|\Psi^\mp\right\rangle$	$\left\|\Psi^-\right\rangle$

Measurement: A and B measure the state of their target particle ($\sigma_z^{A_2}$ and $\sigma_z^{B_2}$) and broadcast their results. If the results are the same, they keep the source particles, and otherwise they discard them. This amounts to taking only the states which had as a result $\Psi^\pm$ in the target bits(i.e. only considering the first four rows of the above table). Using the table, one sees that this is

equivalent to projecting the initial states onto the subspace in which either both the sources and the targets are Φ states or both Ψ states. Let us calculate the projection of the new density operator onto the state $|\Phi^+\rangle$ in the case the measurements were successful. We have the following possibilities:
* With probability F^2 the initial state was $|\Phi^+\rangle_1 |\Phi^+\rangle_2$. In this case the final state of the source will be the desired one.
* With probability $(1-F)^2/9$ the initial state was $|\Phi^-\rangle_1 |\Phi^-\rangle_2$. In this case the final state of the source will be the desired one.
* With probability $F(1-F)/3$ the initial state was $|\Phi^-\rangle_1 |\Phi^+\rangle_2$. With the same probability the initial state was $|\Phi^+\rangle_1 |\Phi^-\rangle_2$. In both cases, the final states will not be the desired one.
* The other 4 possible initial state, products of $|\Psi^\pm\rangle_1$ with $|\Psi^\pm\rangle_2$ have a probability $(1-F)^2/9$ each.
Thus, the probability of having at the end of the process the state $|\Phi^+\rangle_1$ is

$$F' = \frac{F^2 + (1-F)^2/9}{F^2 + 2F(1-F)/3 + 5(1-F)^2/9}. \tag{5.11}$$

For $1 > F > 1/2$, we have that $F' > F$. Therefore, the fidelity after this operation increases.
(4) Unilateral Rotation: One of the observers applies the operation σ_y to his source particle, which transforms $|\Phi^+\rangle \to |\Psi^-\rangle$. Then, one can start again with the procedure, but starting with a fidelity $F' > F$.

Chapter 6

ERROR CORRECTION

6.1 Introduction

• Errors: In any computation (classical and quantum) or during storing of information there will be errors. One way to fight against these errors is to improve the hardware and make it better. However, this is expensive, and not always possible. Shannon realized that instead if trying to avoid the errors it is much better to correct them. This is done by giving redundant information, and using this extra information to find out if an error occur.
• Types of errors: one can distinguish two kinds of errors: (1)Memory errors: Those that occur to the information that is stored, regardless of whether an operation takes place or not; (2)Operation errors: Those that occur during an operation.
Here we will concentrate on memory errors, since the corresponding correction procedures are easier to understand. On the other hand, they plat an important role not only in quantum computation, but also in quantum communication and information. Once one know how memory errors can be corrected, with some modifications one can understand how to correct operation errors. We will first revise the most straightforward way of correcting errors in a classical computer, and then we will show how to do it in a quantum computer.

6.2 Simple Classical Error Correction Codes

• Errors: Imagine that one want to store a single bit for a time t (We will call this bit a *bit*). We do not know what is the state of the bit (0 or 1). Let us denote by P_τ the probability that one occurs in a time interval τ; that is, the probability that the bit flips (if it was 0 then it changes to 1 and viceversa). If $p_\tau \simeq 1$ there will be problems in achieving the goal.
• Code Words: One way to correct the errors is based on what is called *redundant coding.* This consists of using three bits to store the logical bit. That is, we

encode the information such that if the logical bit is 0 the three bits are 0, and if it is 1, the three bits are 1:

$$0_L \equiv 000, \quad 1_L \equiv 111. \tag{6.1}$$

There logical qubits are called *code words*.
• Errors Probabilities Before The Correction: After at time τ, we will have
(1) Probability of no errors: $(1 - P_\tau^3$ (for example, if we had initially 000, after the time τ it is 000).
(2) Probability of error in one bit: $3P_\tau(1 - P_\tau)^2$ (for example, if we had initially 000, after the time τ it is 010 or 001).
(3) Probability of error in one bit: $3P_\tau^2(1 - P_\tau)$ (for example, if we had initially 000, after the time τ it is 011, 101 or 110).
(4) Probability of error in one bit: P_τ^3 (for example, if we had initially 000, after the time τ it is 111).
• Errors Correction: The error correction consists of measuring if the three bits are in the same state or not. If they are in the same state, then we do nothing. If they are a different state, we use majority vote to change the bit that is different. For example, if we have the first and the third bit are equal and the second is different (010 or 101), we flip the second bit (000 and 111, respectively).
• Error Probabilities After The Correction: After the correction we will have the correct state with a probability $P_\tau^c = (1 - P_\tau)^3 + 3P_\tau(1 - P_\tau)^2 = 1 - 3P_\tau^2 + 2P_\tau^3$. Thus, one gains if $P_\tau^c > 1 - P_\tau$, that is, if (roughly) $P_\tau > 1/2$.
• Correction For Long Times: If one wants to keep the state for very long time t, one has to perform that $P_\tau = c\tau$ for time τ sufficiently short. Let us divide t in N intervals of duration $\tau = t/N$. For N sufficiently large, the probability of having the correct state after performing the correction after the time t will be

$$P_\tau^c = \left[1 - 3\left(\frac{ct}{N}\right)^2 + 2\left(\frac{ct}{N}\right)^3\right]^N. \tag{6.2}$$

For $N \ll 3(ct)^2$ this probability can be made as close to one as desired. This is known as the Zone effect.
• Generalizations: One can generalize this to the case in which one wants to store k logical bits and allow for errors in t bits. For example, encoding

$$0_L \equiv 00000, \quad 1_L \equiv 11111, \tag{6.3}$$

one can allow for two errors.

6.3 Simple Quantum Error Correction Codes

6.3.1 Spin Flip

• Errors: Imagine that one wants to store a single quantum bit in an unknown state

$$c_0 |0\rangle + c_1 |1\rangle \tag{6.4}$$

for a time t (we will call this bit a *logical qubit*). Let us assume that after at time τ with a probability $1-P_\tau$ the qubit remains intact and that with a probability P_τ it changes to

$$|\psi\rangle = c_0 |1\rangle + c_1 |0\rangle . \tag{6.5}$$

This error is called spin flip, and it can be represented by the action of σ_x onto the state of the qubit. As before, if $p_\tau \simeq 1$ there will be problems in achieving the goal.

• Code Words: One can correct the above error by using *redundantcoding*. For example, one can *encode* the state of the logical qubit in 3 qubits as

$$0_L \equiv 000, \quad 1_L \equiv 111, \tag{6.6}$$

so that the state (6.4) of the three qubits becomes

$$|\Psi\rangle = c_0 |0\rangle_L + c_1 |1\rangle = c_0 |000\rangle + c_1 |1\rangle_L . \tag{6.7}$$

The subspace spanned by the states (6.6) is called the subspace of code words.

• Error Probabilities Before The Correction: After a time τ, we will have

(1) Probability of no errors: $(1-P_\tau^3$ (the state will be $|\Psi\rangle_L$).

(2) Probability of error in one bit: $3P_\tau(1-P_\tau)^2$ (the state may be $\sigma_x^1 |\Psi\rangle_L , \sigma_x^2 |\Psi\rangle_L$, or$\sigma_x^3 |\Psi\rangle_L$).

(3) Probability of error in one bit: $3P_\tau^2(1-P_\tau)$ (the state may be $\sigma_x^1\sigma_x^2 |\Psi\rangle_L , \sigma_x^1\sigma_x^3 |\Psi\rangle_L$, or$\sigma_x^2\sigma_x^3 |\Psi\rangle_L$).

(4) Probability of error in one bit: P_τ^3 (the state may be $\sigma_x^1\sigma_x^2 sigma_x^3 |\Psi\rangle_L$).

• Error Correction: The error correct takes place as in the classical case. It consists of measuring if the three bits are in the same state or not. If they are in the same state, then we do nothing. If they are a different state, we use majority vote to change the bit that is different. All these measurements have to be performed without destroying the superposition. This can be done as follows: first we measure the projector $P = |000\rangle\langle 000| + |111\rangle\langle 111|$. If we obtain 1, then we leave the qubits are they are. If we obtain 0 then we measure the projector $P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$; if we obtain 1 we apply the local unitary operator σ_x^1 and if not we proceed. We measure $P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$; if we obtain 1 we apply the local unitary operator σ_x^2 and if not we apply the operator σ_x^3 (note that if we measure the operator P_3 we would obtain 1 with probability 1). As a result, if there was either no error or one error, it will be corrected. If there were two or more errors, they will not be corrected.

• Error Probabilities After The Correction: After the correction we will have the correct state with a probability $P_\tau^c = (1-P_\tau)^3 + 3P_\tau(1-P_\tau)^2 = 1 - 3P_\tau^2 + 2P_\tau^3$. Thus, one gains if $P_\tau^c < 1 - P_\tau$, that is, if (roughly) $P_\tau < 1/2$.

• Correction For Long Times: One can use the Zone effect to keep one state unperturbed for an arbitrarily long time. One can also generalize to the case of soring more k logical qubits and allowing for errors in t qubits.

6.3.2 Phase Flip

• Errors: Suppose that now the error corresponds to a phase flip

$$|\psi\rangle = c_0 |0\rangle - c_1 |1\rangle . \tag{6.8}$$

This error is called spin flip, and it can be represented by the action of σ_z onto the state of the qubit.
• Codes: It is convenient to use the eigenstates of σ_x, $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ instead of $|0\rangle$ and $|1\rangle$. The reason is that the operator that creates the error σ_z transforms $|+\rangle \longleftrightarrow |-\rangle$. Thus, the problem is equivalent to the spin flip analyzed in the previous version. In particular, the right encoding is now

$$|0\rangle_L = |+++\rangle\,, \quad |1\rangle_L = |---\rangle\,. \tag{6.9}$$

• Bit ANd Phase Shift: If the error corresponds to a phase and spin flip

$$|\psi\rangle = c_0 |0\rangle - c_1 |1\rangle . \tag{6.10}$$

we can use the same code as for the spin flip.
• Many Errors: If more than one kind of errors $(\sigma_x, \sigma_y, \sigma_z)$ and possible, then the previous codings do not correct them.

6.4 Quantum error correction codes: general case

• Goal: We want to preserve the state of k qubits against arbitrary errors in t different qubits. To do that we encode the *k logical qubits* in n qubits. We have to find the code words that achieve this task, as well as the error correction procedure.
• arbitrary Errors: An arbitrary error in the j-th qubit correspond to the application of an arbitrary operator to that qubit. Note that any arbitrary operator acting on a qubit (a two dimensional Hilbert space) can be written as a linear combination of the identity I^j and the Pauli operators $\sigma_x^j, \sigma_y^j, \sigma_z^j$,since, as we have seen, these operators form a basis. Thus, the operator A corresponding to an arbitrary error on the qubits $j_1, j_2, ..., j_l$ can be written as a linear combination

$$A_l = \sum_{\alpha_1} \sum_{\alpha_2} \cdots \sum_{\alpha_l} c_{\alpha_1,\alpha_2,\ldots,\alpha_l} E^{j_1,j_2,\ldots,j_l}_{\alpha_1,\alpha_2,\ldots,\alpha_l}. \tag{6.11}$$

where the index $\alpha_i = 0,\ x, y, z$, the c's are complex numbers, and we have defined

$$E^{j_1,j_2,\ldots,j_l}_{\alpha_1,\alpha_2,\ldots,\alpha_l} \equiv \sigma^{j_1}_{\alpha_1} \sigma^{j_2}_{\alpha_2} ... \sigma^{j_l}_{\alpha_l}. \tag{6.12}$$

Here, $\sigma_0^j \equiv I^j$ for the sake of a compact notation. In particular, $E_{00\ldots0}$ is the identity.
• Error Correction: The idea of the error correction scheme is as follows:

(1) Code words: We encode k logical qubits in n qubits. The subspace of code words $\mathcal{H}_L$ has dimension 2^k, whereas the Hilbert space $\mathcal{H}$ of all the qubits has dimensions 2^n. Each of the possible E operators defined in (6.12) transforms $\mathcal{H}_L$ into a subspace

$$\mathcal{H}^{j_1,j_2,\ldots,j_l}_{\alpha_1,\alpha_2,\ldots,\alpha_l} \subset \mathcal{H} \tag{6.13}$$

of dimension 2^k. The subspace of code words has to be such that all these subspaces are mutually orthogonal. This condition imposes a minimum bound (the quantum Hamming bound) to the number of qubits needed, since all these orthogonal subspaces have to fit in $\mathcal{H}$. Let us calculate this bound. To do that we have to count the number of different E operators that have t or less Pauli operators acting on the n qubits. We count first the number of those operators that contain l Pauli operators, and then sum these numbers for $l = 0$ up to $l = t$. For the first part of the problem we find that there are $3^l n!/[l!(n-l)!]$ operators, since there are $n![l!(n-l)!]$ combinations of l qubits within n qubits, and in each of the l qubits there are three possible Pauli operators. Thus, the quantum Hamming bound is

$$2^k \sum_{l=0}^{t} 3^l \binom{n}{l} < 2^n. \tag{6.14}$$

For $k = 1$ the minimum n is 5.

(2) General Procedure: First, one measures all the projectors on the subspaces (6.13). Since these subspaces are orthogonal to each other, only the measurement of one projector will give 1, and the state of the system will be projected onto the corresponding subspace $\mathcal{H}^{j_1,j_2,\ldots,j_l}_{\alpha_1,\alpha_2,\ldots,\alpha_l}$. Then one applies the unitary operator $E^{j_1,j_2,\ldots,j_l}_{\alpha_1,\alpha_2,\ldots,\alpha_l}$. The first part of the procedure corresponds to the detection of the error, whereas the second one corresponds to the correction. Let us prove that this indeed corrects any error of the form (6.11) for $l \leq t$. Given any state $|\psi\rangle$ in the code word subspace, if an error of the form (6.11) occurs, the state will be $A_l\,|\psi\rangle$, which is in the direct sum of all the subspaces (6.13). The measurement will project the state onto one of these subspaces, so that the state after the measurement will be

$$E^{j_1,j_2,\ldots,j_l}_{\alpha_1,\alpha_2,\ldots,\alpha_l}\,|\psi\rangle\,. \tag{6.15}$$

The correction will produce the right state $|\psi\rangle$ since $(E^{j_1,j_2,\ldots,j_l}_{\alpha_1,\alpha_2,\ldots,\alpha_l})^2 = 1$.

• Statement of the problem: The problem of finding general codes for correction of t errors in n qubits reduces to finding the right code word subspace of dimension 2^k so that all the operators E (6.12) lead to mutually orthogonal subspaces.

6.4.1 Code Stabilizers

• Idea: In this subsection we will see how to construct codes that correct errors in t different qubits, when one encodes k logical qubits into n qubits (provided the quantum Hamming bound is fulfilled).

• Properties of Pauli operators: Let us review some properties of the Pauli operators that we will need:

$$[\sigma_x^i, \sigma_y^i] = 2i\sigma_z^i, \quad \{\sigma_x^i, \sigma_y^i\} = 0, \tag{6.16a}$$

$$[\sigma_y^i, \sigma_z^i] = 2i\sigma_x^i, \quad \{\sigma_y^i, \sigma_z^i\} = 0, \tag{6.16b}$$

$$[\sigma_z^i, \sigma_x^i] = 2i\sigma_y^i, \quad \{\sigma_z^i, \sigma_x^i\} = 0. \tag{6.16c}$$

• Group of possible operators: Let us consider the set $\mathcal{G}_1$ of all possible operators formed as products of Pauli operators. For example, the operators

$$G_1 = \sigma_x^1\sigma_y^3\sigma_z^4\sigma_x^5, \tag{6.17a}$$

$$G_2 = \sigma_y^1\sigma_x^2\sigma_y^3\sigma_y^5, \tag{6.17b}$$

$$G_3 = \sigma_x^1\sigma_y^2\sigma_x^3\sigma_x^4\sigma_x^5, \tag{6.17c}$$

belong to $\mathcal{G}_1$. This set has 4^n elements. We denote by $\mathcal{G}_+ \equiv \mathcal{G}_1 \cup (-\mathcal{G})$ and by $\mathcal{G}_- \equiv i\mathcal{G}_+$ (i is the imaginary number). The set $\mathcal{G} \equiv \mathcal{G}_+ \cup \mathcal{G}_-$ is a finite group of order 4^{n+1}. This sets have the following properties:
(1) Given that $(\sigma_\alpha^i)^2 = 1$, each of the elements of $\mathcal{G}_+$ squares to $+1$. They are hermitian and unitary since each of them is a product of hermitian and unitary operators that commute (The elements of $\mathcal{G}_-$ square to -1, are antihermitian and unitary).
(2) If $A, B \in \mathcal{G}$, then $AB = \pm BA$; that is, either $[A, B] = 0$ or $\{A, B\} = 0$. For example,

$$\begin{aligned} G_1G_2 &= (\sigma_x^1\sigma_y^1)(\sigma_x^2)(\sigma_y^3\sigma_y^3)(\sigma_z^4)(\sigma_x^5\sigma_y^5) \\ &= (-\sigma_y^1\sigma_x^1)(\sigma_x^2)(\sigma_y^3\sigma_y^3)(\sigma_z^4)(-\sigma_y^5\sigma_x^5) \\ &= G_2G_1. \end{aligned}$$

$$\begin{aligned} G_1G_3 &= (\sigma_x^1\sigma_z^1)(\sigma_y^2)(\sigma_y^3\sigma_x^3)(\sigma_z^4\sigma_x^4)(\sigma_x^5\sigma_y^5) \\ &= (-\sigma_z^1\sigma_x^1)(\sigma_y^2)(-\sigma_x^3\sigma_y^3)(-\sigma_x^4\sigma_z^4)(\sigma_x^5\sigma_x^5) \\ &= -G_3G_1. \end{aligned}$$

In particular, $[A, B] = 0$ if the number of instances where two different spin operator appear for a qubit is even and $A, B = 0$ if this number is odd.
• Code words: Let us denote by $\mathcal{H}_L$ the subspace code words. It has dimension 2^k.
• Stabilizer: Let us denote by S the *stabilizer* of $\mathcal{H}_L$, i.e. the set of operators belonging to $\mathcal{G}$ which leave invariant the states of $\mathcal{H}_L$,

$$S = \{M \in \mathcal{G} s.t. M\left|\psi\right\rangle = \left|\psi\right\rangle \forall \left|\psi\right\rangle \in \mathcal{H}_L\}. \tag{6.18}$$

Any stabilizer must have the following properties:
(1) Group: S is a subgroup of $\mathcal{G}$ (i.e. $M, N \in S$, then $MN \in S$). The proof is very simple: for any $\left|\psi\right\rangle \in \mathcal{H}_L, MN\left|\psi\right\rangle = M\left|\psi\right\rangle = \left|\psi\right\rangle$.

(2) Abelian: S is abelian; that is if $M, N \in S$, then $[M, N] = 0$. The proof is simple, since according to the properties of $\mathcal{G}$, either $[M, N] = 0$ or $M, N = 0$. However, we have $[M, N] |\psi\rangle = 0, M, Nket\psi = 2 |\psi\rangle$ for all $|\psi\rangle \in \mathcal{H}_L$.
(3) Its elements square to one: According to the properties of $\mathcal{G}$, its elements either square to $+1$ or to -1. Since $M^2 |\psi\rangle = |\psi\rangle$ for all $|\psi\rangle \in \mathcal{H}_L$, then $M^2 = 1$.
(4) Isomorphic to $(Z_2)^a$: S is an abelian group whose elements square to one. Therefore it has to be isomorphic to $(Z_2)^a$ for a given a. $(Z_2)^a$ is the direct product of the a groups of order 2 [Z_2 is the group whose elements are 0 and 1 with the operation XOR (equivalent to addition mod (1))].
(5) Generations: Given this isomorphism, these exist a set of a elements of S that: (i) they generate it (that is, all the elements can be written as products of these operators); (ii) they are minimal (i.e. there exists no other set of elements which contains less number of operators and generates S). Let us denote them by $M_1, M_2, ...M_a$.
(6) Dimension of $\mathcal{H}_L$: The dimension of $\mathcal{H}_L$ must be 2^{n-a}, where a is the number of generators of S. This can be seen as follows. All the generators commute, and have eigenvalues ± 1. Therefore one can divide the Hilbert space $\mathcal{H}$ into orthogonal subspaces while are eigenspaces of all the generators. Since each subspace is characterized by the eigenvalues of all the generators, there must be 2^a subspaces. THe dimension of each subspace is therefore 2^{n-a}. The subspace corresponding to all the eigenvalues equal to $+1$ is precisely $\mathcal{H}_L$. Since on the other hand dim $(\mathcal{H}_L = 2^k)$, we have $a = n - k$.
• Errors: Let us denote by E_1 and E_2 two different operators of the form (6.12). According to the above discussion, error correction will be possible if and only if $E_1 |\psi\rangle$ is original to $E_2 |\phi\rangle$ for all $|\psi\rangle, ket\phi \in \mathcal{H}_L$. This is automatically satisfied if the operator E_1E_2 anticommutes with at least one element M of the stabilizer S. To show this, we write

$$\begin{aligned}\langle\phi| E_1E_2 |\psi\rangle = \langle\phi| E_1E_2M |\psi\rangle = - \langle\phi| ME_1E_2 |\psi\rangle \\ = - \langle\phi| E_1E_2 |\psi\rangle .\end{aligned} \tag{6.19}$$

and therefore $\langle\phi| E_1E_2 |\psi\rangle = 0$. Thus, the problem reduces to finding a subspace $\mathcal{H}_L$ and a stabilizer S so that every non trivial operator in $\mathcal{G}$ of the length less than or equal $2t$ anticommutes with some members in S.
• Procedure: The problem reduces to finding a subspace $\mathcal{H}_L$ and a stabilizer S so that every nontrivial operators in $\mathcal{G}$ of length less than or equal to $2t$ anticommutes with some members in S. To do that, one first finds an abelian group S composed of products of Pauli operators, so that all the errors up the length $2t$ anticommute with some element of it. Once the stabilizer is known, one can find $\mathcal{H}_L$, i.e. the code words.
(1) For a given $M \in \mathcal{G}$, we define the function $f_M : \} \rightarrow Z_2$ as

$$f_M(N) = \begin{cases} 0 \; if \; [M, N] = 0, \\ 1 \; if \; \{M, N\} = 0, \end{cases} \tag{6.20}$$

If S is generated by $M_1, M_2, ..., M_a (a = n - k)$, we define the function $f : \mathcal{G} \to (Z_2)^a$ by

$$f(N) = [f_{M_1}(N), f_{M_2}(N), ..., f_{M_a}(N)]. \tag{6.21}$$

In the following we will write $F(N)$ as an a-bit binary string. For example, $F(I) = 000...0$ when $I = I^1 I^2 ... I^n$ is the identity.
(2) We wish to pick S so that $f(E)$ is non-zero for all E up to length $2t$. Writing $E = E_1 E_2$, where E_1, E_2 have length t or less, we have that $f(E) \neq 0$ iff $f(E_1) \neq f(E_2)$. Therefore we need to peak S so that $f(E_i)$ is different for each E_i of the length t or less (6.12).
(3) We can find the generators by choosing an a-bit number $\neq 0$ for each possible error F of length t or smaller. Note that the assignation of these numbers cannot be completely arbitrary since the homomorphism f fulfills some conditions. For example, $f(sigma_y^i) =$XOR$[f(\sigma_x^i), f(\sigma_z^i)]$.
- How to determine $\mathcal{H}_L$: Once the generators are known, one can take one state $|m\rangle$ (in binary notation) and construct the state

$$|\psi\rangle \propto \sum_{M \in S} M |m\rangle . \tag{6.22}$$

If the results in non zero, this state belongs to $\mathcal{H}_L$, since if we apply any operator $M' \in S$, the to $|\psi\rangle$ this corresponds to reordering the sum (since S is a finite group). Thus, one can try with the different states of the basis $|00...00\rangle , |00...01\rangle$ etc until one finds k orthogonal states.

6.4.2 Example: correction of one error in one qubit

- Problem: We consider the case $k = t = 1, n = 5$. Thus $a = n - k = 4$.
- Errors: The 16 possible E operators are the Pauli operators (3 for each qubit) plus the identity.
- a-Bit numbers: We have to choose an 4-bit number for each E Operator. THese number must be different, are $f(\sigma_y^i) =$XOR$[f(\sigma_x^i), f(\sigma_z^i)]$. For example, we can choose

$$\begin{aligned} &\sigma_x^1 : 0110, \sigma_z^1 : 1000, \sigma_y^1 : 1110, \\ &\sigma_x^2 : 0001, \sigma_z^2 : 0100, \sigma_y^2 : 0101, \\ &\sigma_x^3 : 0111, \sigma_z^3 : 1010, \sigma_y^3 : 1101, \\ &\sigma_x^4 : 1011, \sigma_z^4 : 0010, \sigma_y^4 : 1001, \\ &\sigma_x^5 : 0011, \sigma_z^5 : 1100, \sigma_y^5 : 1111, \end{aligned} \tag{6.23}$$

- Generators: The first digit to the a-bit numbers corresponds to the first generators, the second to the second, etc. Since the first digit of σ_x^1 is 0, $[M_1, \sigma_x^1] = 0$; on the other hand, since the first digit of σ_y^1 are 1, then they anticommute with M_1. Thus, M_1 contains σ_x^1. As a general rule, the r-th generator contains the identity at the position of the i-th qubits. If not, it will contain the operator which has a 0. We find:

$$M_1 = \sigma_x^1\sigma_x^3\sigma_x^4\sigma_x^5, \tag{6.24a}$$
$$M_2 = \sigma_x^1\sigma_x^2\sigma_z^3\sigma_x^5, \tag{6.24b}$$
$$M_3 = \sigma_z^1\sigma_y^3\sigma_y^4\sigma_z^5, \tag{6.24c}$$
$$M_4 = \sigma_z^2\sigma_z^3\sigma_z^4\sigma_z^5. \tag{6.24d}$$

All of them commute.

6.5 Decoherence

• Coupling to an environment: The above error correction schemes word in the presence of (undesired) coupling to the environment which lead to decoherence.
• Single qubit environments: We assume for simplicity that each of the qubit is coupled to an independent environment. Thus, the evolution of the i-th qubit and environment, in general, will be given by

$$|0\rangle_i |E\rangle_i \to |0\rangle_i |E_{00}\rangle_i + |1\rangle_i |E_{01}\rangle_i \,, \tag{6.25a}$$
$$|1\rangle_i |E\rangle_i \to |0\rangle_i |E_{10}\rangle_i + |1\rangle_i |E_{11}\rangle_i \,, \tag{6.25b}$$

where $|E_{ij}\rangle_i$ are unnormalized states of the environment. The operator accomplishing this transformation can be written, in general, as

$$\begin{aligned} U^i =& \alpha^i 1^1 \otimes U_0^i + \epsilon_1^i \sigma_x^i \otimes U_1^i \\ &+ \epsilon_2^i \sigma_y^i \otimes U_2^i + \epsilon_3^i \sigma_z^i \otimes U_3^i, \end{aligned} \tag{6.26}$$

where the U's are unitary operators acting on the environment, and α^i and ϵ_{123}^i are constant numbers. We will consider that the time is sufficiently short so that all $\alpha^i \simeq 1$ and $\epsilon_{123}^i \ll 1$.
• Expansion: The state of the qubits after some interaction time can be expanded in terms of the epsilons as follows:

$$\begin{aligned} U|\psi\rangle|E\rangle = \prod_{i=1}^n U^i |\psi\rangle|E\rangle = [\prod_{i=1}^n \alpha^i 1^i U_0^i \\ + \sum_{j=1}^n \epsilon_1^j \sigma_x^j U_1^j \prod_{j\neq i} \alpha^i 1^i U_0^i + \sum_{j=1}^n \epsilon_2^j \sigma_y^j U_2^j \prod_{j\neq i} \alpha^i 1^i U_0^i \\ + \sum_{j=1}^n \epsilon_3^j \sigma_x^j U_3^j \prod_{j\neq i} \alpha^i 1^i U_0^i + o(\epsilon^2)] |\psi\rangle|E\rangle \,. \end{aligned} \tag{6.27}$$

• Error correction: The error correction explained in the previous Section will project the state onto only one of the terms of the expression. The state of the environment will therefore factorize, and therefore all the analysis made before remains valid.