Density operator; ρ

Supose we have a generator of quantum (orthogonal!) states $\{|\varphi_i\rangle\}_{i=0}^{N}$, each of them with a probability $\{p_i\}_{i=0}^{N}$. For a finite number N. Notice that

$$p_i > 0 \quad \forall i \in \{0, \dots, N\}.$$

Since the case $p_j = 0$ is discarted because the generator would never produce $|\varphi_j\rangle$, but $\{|\varphi_i\rangle\}_{i=0}^{N}$ is the set of possible outcomes, subsequently $|\varphi_j\rangle \notin \{|\varphi_i\rangle\}_{i=0}^{N}$, contradiction!

in this context we define the density as

$$\rho = \sum_{i=0}^{N} p_i |\varphi_i\rangle\langle\varphi_i|$$

Pure states!

a density matrix is said to represent a pure state iff,

- ρ is a projector (i.e. $\rho^2 = \rho$) with rank -1.
- $tr(\rho^2) = 1$.

Simple example: a generator provides 2 orthogonal states, $|\varphi_1\rangle$ and $|\varphi_2\rangle$ with equal probability

$$\rho = \frac{1}{2}(|\varphi_1\rangle\langle\varphi_1| + |\varphi_2\rangle\langle\varphi_2|)$$

$$= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \leftarrow \text{pure states!}$$

Now let us supose the generator produces only 1 state in quantum superposition $|\varphi\rangle = \frac{1}{\sqrt{2}}(|\varphi_1\rangle + |\varphi_2\rangle)$, now the density matrix is nothing but,

$$\underset{\substack{\uparrow \\ \text{probability} \\ 1}}{\rho} = |\varphi\rangle\langle\varphi| = \frac{1}{2}(|\varphi_1\rangle + |\varphi_2\rangle)(\langle\varphi_1| + \langle\varphi_2|)$$

$$= \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \leftarrow \text{mixed states!}$$

Note: the case of infinite dimensions

$$\rho = \sum_i p_i |\varphi_i\rangle\langle\varphi_i| \rightsquigarrow \rho = \int p_i |\varphi\rangle\langle\varphi| dx$$

Quite complex!

We will stick in the fine case.

Projective measurement / POVM's.

Given a set of states $\{|\varphi_i\rangle\}_{i=0}^{N}$ let us make the usual operation Π_m, a meaurement with the particularity that.

$$0 \leq \langle \Pi_m \rangle_{\varphi_i} \leq 1.$$

Notice this kind of projector can always be constructed by a positive-definite operator P, (i.e. $\langle P \rangle_{\varphi_i} \geq 0 \; \forall i$). we define

$$\Pi = \frac{P}{\lambda_{max}} \leftarrow \text{highest eigenvalue of } P. \quad //$$

Therefore we define the probability of "m" as

$$p(m) = \sum_i p_i \langle\varphi_i|\Pi_m|\varphi_i\rangle$$

for a given projector Π_m. //

Thus

$$p(m) = \sum_i p_i \langle\varphi_i|\Pi_m|\varphi_i\rangle$$

$$= \sum_i p_i \, tr(\langle\varphi_i|\Pi_m|\varphi_i\rangle)$$

$$= tr\left(\sum_i p_i \langle\varphi_i|\Pi_m|\varphi_i\rangle\right)$$

$$= tr\left(\left[\sum_i p_i |\varphi_i\rangle\langle\varphi_i|\right]\Pi_m\right)$$

$$= tr(\rho\Pi_m) = tr(\Pi_m\rho)$$

this is the kind of expression we want to work with!

If we want to mull it over a bit we can also extend this definition to the POVM's one. a set of positive definite operators is said to be a POVM iff $\{E_i\}_{i=0}^{N}$

$$\sum_{i=0}^{N} E_i = \mathbb{I}d \quad //$$

This condition is kind a relatet to the probabilities to add up to 1.

Grahm matrix, such a straightforward object at first glance, but super usefull since contains a lot of information of our system (if not all)

Given a set of states $\{|\varphi_i\rangle\}_{i=1}^{N}$, not necessarely orthogonal we define the Grahm (G) matrix as the $N \times N$ matrix such that $G_{ij} = \langle\varphi_i|\varphi_j\rangle$ or equivalently

$$G = \sum_i \sum_j \langle\varphi_i|\varphi_j\rangle |i\rangle\langle j| \quad //$$

orthogonal basis!

Let us supose we have a quantum states generator (☆). We know ☆ to produduce just a certain ammount of states with $\{\rho_i\}_{i=1}^{N}$ density matrices, each of them with a prior probability of $\{\eta_i\}_{i=1}^{N}$

For the time being our goal is to compute the probability of guessing the state right (identification)

It is natural to wander which is the the probability of observing an outcome that points out at a certain ρ_j and indeed have ρ_j. The answer is

$$P\left(\underset{\rho_j}{\text{measure}} \,\middle|\, \underset{\rho_j}{\text{have}}\right) = tr(E_j\rho_j)$$

furthermore, the probability of ☆, to produce ρ_j is η_j, therefore the probability of guessing ρ_j right is

$$P\left(☆ \underset{\rho_j}{\text{produce}}\right) = \eta_j$$

by definition. Therefore the probability of guessing, ρ_j, right is nothing but,

$$P\left(\underset{\rho_j \text{ right}}{\text{guessing}}\right) = P\left(\underset{\rho_j}{\text{measure}} \,\middle|\, \underset{\rho_j}{\text{have}}\right) P\left(☆ \underset{\rho_j}{\text{produce}}\right)$$

$$= tr(E_j\rho_j)\,\eta_j \quad \{E_i\} \text{ POVM}$$

Finally, the probability of having a good guess is trivially the sum over "j" of guessing ρ_j correctly i.e.

$$P_{success} = \sum_{j=1}^{N} \eta_j \, tr(E_j\rho_j). \quad //$$

Since our goal is to maximize the success probability we seek the set of POVMs $\{E_i\}$ such that,

$$P_{success} = \max_{\{E_i\}} \sum_{i=1}^{N} \eta_i \, tr(E_i\rho_i)$$

Here we might take two appraches be sure of each guess (0-error) or maximizing the success probability disregarding the error porobability.

Let us begin, we have a set of states $\{|\psi_i\rangle\}_{i=1}^{N}$, each of them wit a prior probability $\{\eta_i\}$

The Grahm matrix is nothing but

$$\mathcal{G}_{ij} = \sqrt{\eta_i}\sqrt{\eta_j}\langle\psi_i|\psi_j\rangle \leftarrow \text{we must take into account the priors}$$

Notice that,

$$x^{\dagger}\mathcal{G}x = \sum_{ij} x_i^{\dagger} x_j \langle\psi_i|\psi_j\rangle$$

$$= \sum_{ij} \langle x_i\psi_i | x_j\psi_j\rangle \quad x_i, x_j \text{ is an orthogonal basis}$$

$$= \left\langle \sum_i x_i\psi_i \,\middle|\, \sum_j x_j\psi_j \right\rangle$$

$$= \sum_i \langle x_i\psi_i | x_i\psi_i\rangle$$

$$\geq 0 \leftarrow \text{Positive defined}$$

The Positive definition allow us to decompose $\mathcal{G}$ into,

$$\mathcal{G} = S^{\dagger}S$$

The "square root" of $\mathcal{G}$.

Notice this decomposition is not unique since perhaps we define $S' = \mathcal{U}S$, where $\mathcal{U}$ is an unitary matrix, we observe

$$(S')^{\dagger}S' = (\mathcal{U}S)^{\dagger}\mathcal{U}S = S^{\dagger}\mathcal{U}^{\dagger}\mathcal{U}S$$

$$= S^{\dagger}S = \mathcal{G}.$$

S' is a square root of $\mathcal{G}$ too.

However we always can find $\mathcal{U}$ such that $S' = \mathcal{U}S$ is $(S')^{\dagger} = S'$ hermitic!

We denote $S' = \mathcal{G}^{1/2}$.

Let Ω be

$$\Omega = \sum_i \eta_i \rho_i \geq 0 \leftarrow \text{positive defined!}$$

We can define the Square root measurement as

$$E_i = \eta_i \, \Omega^{-1/2} \rho_i \Omega^{-1/2}.$$