IV. States, Observables, and Statistics

In this chapter we turn to how measurements in quantum computing are mathematically defined and statistically interpreted. Throughout we assume $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ to be a complex Hilbert space which is separable and often even finite-dimensional. We recall from (II.47) that quantum states are represented by density matrices $\rho \in \mathcal{DM}(\mathcal{H})$, where

$$\mathcal{DM}(\mathcal{H}) \;=\; \big\{\rho \in \mathcal{L}^1(\mathcal{H}) \;\big|\; \rho = \rho^* \geq 0\,,\; \mathrm{Tr}(\rho) = 1\big\} \;\subseteq\; \mathcal{L}^1(\mathcal{H})\,, \tag{IV.1}$$

and that observables are represented by bounded self-adjoint operators $A \in \mathcal{SA}(\mathcal{H})$, where

$$\mathcal{SA}(\mathcal{H}) \;=\; \big\{A \in \mathcal{B}(\mathcal{H}) \;\big|\; A \;=\; A^*\big\} \;\subseteq\; \mathcal{B}(\mathcal{H})\,. \tag{IV.2}$$

Note that $\mathcal{SA}(\mathcal{H}) \subseteq \mathcal{B}(\mathcal{H})$ is a real, but not a complex, subspace of $\mathcal{B}(\mathcal{H})$.

IV.1. Observables and Resolutions of the Identity

Given a density matrix $\rho \in \mathcal{DM}(\mathcal{H})$, we interpret the expectation value $\langle A\rangle_\rho := \mathrm{Tr}(\rho A)$ of an observable $A \in \mathcal{SA}(\mathcal{H})$ to be the outcome of the measurement of the physical quantity represented by A, e.g., the position of a particle or its spin. *These measurements are the only access to ρ we have.*

Note that $\rho \in \mathcal{DM}(\mathcal{H})$ is determined by the collection $\big(\langle A\rangle_\rho\big)_{A\in\mathcal{SA}(\mathcal{H})} \in \mathbb{R}^{\mathcal{SA}(\mathcal{H})}$ of the measurements of all observables. For if the measuments of two density matrices $\rho, \hat\rho \in \mathcal{DM}(\mathcal{H})$ all coincide then $\mathrm{Tr}\big[(\rho - \hat\rho)A\big] = \langle A\rangle_\rho - \langle A\rangle_{\hat\rho} = 0$, for all $A \in \mathcal{SA}(\mathcal{H})$ which implies that $\rho - \hat\rho = 0$.

We conclude that observables play the same role for states as random variables do for probability measures. A basic mathematical fact of stochastics is that a probability measure is determined by the collection of expectation values of all its random variables, and we may identify the probability measure with this collection. In practise, our access to observables is limited and we have to use some other information to determine the state as precisely as possible.

We now suppose we have a set $\mathcal{A}$ of possible outcomes of a measurement. For simplicity, we assume $\mathcal{A}$ to be finite. It is a good idea to think of $\mathcal{A}$ as to divide the scale of a meter into $|\mathcal{A}|$ sectors. To each of these sectors $a \in \mathcal{A}$ we attribute a positive observable $M_a \geq 0$, and we require that these add to one, $\sum_{a \in \mathcal{A}} M_a = \mathbf{1}_{\mathcal{H}}$. The expectation value $p_a := \mathrm{Tr}(\rho\, M_a)$ of M_a in a given state $\rho \in \mathcal{DM}(\mathcal{H})$ then defines a probability distribution on $\mathcal{A}$. The value p_a is the probability that ρ yields the outcome a. We formalize this now.

Definition IV.1. Let $\big(\mathcal{H}, \langle \cdot | \cdot \rangle\big)$ be a Hilbert space and $\mathcal{A}$ a finite set.

(i) A family $M = \{M_a\}_{a \in \mathcal{A}} \subseteq \mathcal{SA}(\mathcal{H})$ of positive observables $M_a \geq 0$ such that

$$\sum_{a \in \mathcal{A}} M_a \ = \ \mathbf{1}_{\mathcal{H}} \tag{IV.3}$$

is called **resolution of the identity** or **probability operator-valued measure (POVM)**. In this case, $\mathcal{A}$ is the **set of (possible) outcomes $\boldsymbol{a \in \mathcal{A}}$**.

(ii) If $M = \{M_a\}_{a \in \mathcal{A}} \subseteq \mathcal{SA}(\mathcal{H})$ is a resolution of the identity and $M_a = M_a^2$ are orthogonal projections for all $a \in \mathcal{A}$, then M is called **orthogonal** or **sharp**.

Remarks and Examples.

- As indicated above, if we are given a state $\rho \in \mathcal{DM}(\mathcal{H})$ on a Hilbert space $\mathcal{H}$ and a probability operator-valued measure $M = \{M_a\}_{a \in \mathcal{A}} \subseteq \mathcal{B}(\mathcal{H})$ then we define $p : \mathcal{A} \to \mathbb{R}_0^+$ by $p_a := \mathrm{Tr}(\rho\, M_a)$ and observe that p is a probability distribution on $\mathcal{A}$.
- If $\mathcal{H}$ is a Hilbert space of dimension $D = \dim(\mathcal{H}) < \infty$ and $\{f_k\}_{k=1}^D \subseteq \mathcal{H}$ is an ONB then $\big\{ \, |f_k\rangle\langle f_k| \, \big\}_{k=1}^D \in \mathcal{B}(\mathcal{H})$ is an orthogonal resolution of the identity.

In practise, our access to observables is limited and we have to use some other information to determine the state as precisely as possible. One model instance is given as follows:

Let $\{\rho_a\}_{a \in \mathcal{A}} \in \mathcal{DM}(\mathcal{H})$ be a collection of density matrices on a Hilbert space $\mathcal{H}$, where $\mathcal{A}$ is a finite set, $d := |\mathcal{A}| \in \mathbb{N}$, $d \geq 2$. We are given a random distribution of states $\rho \in \{\rho_a\}_{a \in \mathcal{A}}$, where the probability that $\rho = \rho_a$ equals π_a, i.e., $\sum_{a \in \mathcal{A}} \pi_a = 1$ and $0 < \pi_a < 1$ (we may assume strict inequalities w.l.o.g. to avoid trivial cases). Given an observable $B \in \mathcal{SA}(\mathcal{H})$, its expected (w.r.t. π) expectation value is given by

$$\mathbb{E}_\pi[\langle B \rangle_\rho] \ = \ \sum_{a \in \mathcal{A}} \pi_a \, \langle B \rangle_{\rho_a} \ = \ \sum_{a \in \mathcal{A}} \pi_a \, \mathrm{Tr}(\rho_a B) \ = \ \mathrm{Tr}(\rho_\pi \, B) \, , \tag{IV.4}$$

where $\rho_\pi := \sum_{a \in \mathcal{A}} \pi_a \rho_a \in \mathcal{DM}(\mathcal{H})$ is the average density matrix.

We now suppose to be given a resolution of the identity $M = \{M_a\}_{a \in \mathcal{A}} \subseteq \mathcal{SA}(\mathcal{H})$. We relate the expectation value of M_a to the outcome $a \in \mathcal{A}$. More precisely, we define

$$p(a|b) \ := \ \mathrm{Tr}(\rho_b M_a) \tag{IV.5}$$

to be the conditional probability of the outcome a under the condition that the state is ρ_b. The name is justified because, for any $b \in \mathcal{A}$,

$$\sum_{a \in \mathcal{A}} p(a|b) \ = \ \sum_{a \in \mathcal{A}} \mathrm{Tr}(\rho_b \, M_a) \ = \ \mathrm{Tr}(\rho_b) \ = \ 1 \, . \tag{IV.6}$$

That is, $p(a|b)$ is the prediction that the density matrix is ρ_a while it actually is ρ_b. The goal is now to choose the resolution of the identity $M = \{M_a\}_{a \in \mathcal{A}} \subseteq \mathcal{SA}(\mathcal{H})$ such as to maximize the conditional probabilities $p(a|a)$ that predict the density matrix to be ρ_a when this is indeed the case. To aim at a single number to maximize, we weigh these conditional probabilities of correct prediction of ρ_a with the probability of the occurence of ρ_a and define the average probability of making a correct decision

$$\mathcal{P}(M) \ := \ \sum_{a \in \mathcal{A}} \pi_a \, p(a|a) \ = \ \sum_{a \in \mathcal{A}} \pi_a \, \mathrm{Tr}(\rho_a \, M_a) \, . \tag{IV.7}$$

The above goal can now be formulated as the variational problem to determine a resolution of the identity $\hat{M} = \{\hat{M}_a\}_{a \in \mathcal{A}} \subseteq \mathcal{SA}(\mathcal{H})$, such that $\mathcal{P}(\hat{M}) = \mathcal{P}_{\max}$, where

$$\mathcal{P}_{\max} \ := \ \sup \Big\{ \mathcal{P}(M) \ \Big| \ M \in \mathfrak{M}_{\mathcal{A}}(\mathcal{H}) \ \Big\} \tag{IV.8}$$

and the system $\mathfrak{M}_{\mathcal{A}}(\mathcal{H})$ of all resolutions of the identity is given by

$$\mathfrak{M}_{\mathcal{A}}(\mathcal{H}) \ := \ \Big\{ M \in \mathcal{SA}(\mathcal{H})^{\mathcal{A}} \ \Big| \ \forall a \in \mathcal{A} : \ M_a \geq 0 \, , \quad \sum_{a \in \mathcal{A}} M_a = 1 \ \Big\} . \tag{IV.9}$$

Remarks and Examples. Let $\mathcal{A} = \mathbb{Z}_1^d = \{1, 2, \ldots, d\}$, with $d \in \mathbb{N}$, be a finite set and $\Omega = \mathbb{Z}_1^N = \{1, 2, \ldots, N\}$ be the configuration space such that $\mathcal{H} = \ell^2(\Omega) \cong \mathbb{C}^N$ is the Hilbert space of states. Suppose that we have a collection $\{\rho_a\}_{a \in \mathcal{A}} \subseteq \mathcal{DM}(\mathcal{H})$ of mutually commuting density matrices,

$$\forall \, a, b \in \mathcal{A} : \qquad [\rho_a, \rho_b] \ = \ 0 \, . \tag{IV.10}$$

Then there exists an ONB $\{f_k\}_{k \in \Omega} \subseteq \mathcal{H}$ of joint eigenvectors of the ρ_a and nonnegative corresponding eigenvalues $\mu_a(k) \geq 0$ such that $\sum_{k \in \Omega} \mu_a(k) = 1$, for all $a \in \mathcal{A}$, and

$$\forall \, a \in \mathcal{A} : \qquad \rho_a \ = \ \sum_{k \in \Omega} \mu_a(k) \, |f_k\rangle\langle f_k| \, . \tag{IV.11}$$

Given the probability distribution $\pi : \mathcal{A} \to [0, 1]$ for the random choice of $\rho \in \{\rho_a\}_{a \in \mathcal{A}}$, we define $w_a(k) := \pi_a \mu_a(k)$ and

$$\forall \, a \in \mathcal{A} : \qquad W_a \ = \ \sum_{k \in \Omega} w_a(k) \, |f_k\rangle\langle f_k| \, . \tag{IV.12}$$

If $M = \{M_a\}_{a\in\mathcal{A}} \subseteq \mathcal{SA}(\mathcal{H})$ is a resolution of the identity, then

$$\begin{aligned}\mathcal{P}(M) \;&=\; \sum_{a\in\mathcal{A}} \mathrm{Tr}(W_a M_a) \;=\; \sum_{a\in\mathcal{A}}\sum_{k\in\Omega} w_a(k)\,\langle f_k|\, M_a f_k\rangle \\ &\leq\; \sum_{a\in\mathcal{A}}\sum_{k\in\Omega} w_{\max}(k)\,\langle f_k|\, M_a f_k\rangle \;=\; \sum_{k\in\Omega} w_{\max}(k)\,, \end{aligned} \tag{IV.13}$$

using $\sum_{a\in\mathcal{A}} M_a = \mathbf{1}_{\mathcal{H}}$ where

$$\forall\, k\in\Omega: \qquad w_{\max}(k) \;:=\; \max_{a\in\mathcal{A}}\{w_a(k)\}\,. \tag{IV.14}$$

Next we construct a resolution $\hat{M} = \{\hat{M}_a\}_{a\in\mathcal{A}} \subseteq \mathcal{SA}(\mathcal{H})$ of the identity for which $\mathcal{P}(\hat{M}) = \sum_{k\in\Omega} w_{\max}(k)$. To this end we assume to be given a disjoint partition $\{\Omega_a\}_{a\in\mathcal{A}} \subseteq \mathfrak{P}(\Omega)$ of Ω, i.e.,

$$\bigcup_{a\in\mathcal{A}} \Omega_a \;=\; \Omega\,, \qquad \forall\, a,b\in\mathcal{A}\,,\; a\neq b: \quad \Omega_a\cap\Omega_b \;=\; \emptyset\,, \tag{IV.15}$$

and define

$$\forall\, a\in\mathcal{A}: \qquad \hat{M}_a \;=\; \sum_{k\in\Omega} \mathbf{1}[k\in\Omega_a]\,|f_k\rangle\langle f_k|\,. \tag{IV.16}$$

Obviously, $\hat{M}_a \geq 0$. Furthermore, we observe that, due to (IV.15), we have $\sum_{a\in\mathcal{A}} \mathbf{1}[k\in\Omega_a] = 1$, for all $k\in\Omega$, which implies that $\sum_{a\in\mathcal{A}} \hat{M}_a = \mathbf{1}_{\mathcal{H}}$ and hence that $\hat{M}$ is a resolution of the identity, in fact a sharp one.

$$\mathcal{P}(\hat{M}) \;=\; \sum_{a\in\mathcal{A}}\sum_{k\in\Omega} w_a(k)\,\langle f_k|\, M_a f_k\rangle \;=\; \sum_{a\in\mathcal{A}}\sum_{k\in\Omega} w_a(k)\,\mathbf{1}[k\in\Omega_a]\,. \tag{IV.17}$$

For $a\in\mathcal{A}$, we now choose

$$\Omega_a \;:=\; \Big\{ k\in\Omega \;\Big|\; w_a(k) = w_{\max}(k)\,,\;\; \forall\, b\in\mathcal{A}\,,\; b<a: \;\; w_b(k) < w_{\max}(k) \Big\}\,, \tag{IV.18}$$

where the condition that $w_b(k) < w_{\max}(k)$, for $b < a$, ensures that a is the smallest element in $\mathcal{A}$ with $w_a(k) = w_{\max}(k)$ and therefore, for each $k\in\Omega$, there is precisely one $a\in\mathcal{A}$ with $\Omega_a \ni k$. It follows that $\{\Omega_a\}_{a\in\mathcal{A}} \subseteq \mathfrak{P}(\Omega)$ is a disjoint partition of Ω in the sense of (IV.15), and thus $\hat{M}$ is an orthogonal resolution of the identity. Moreover,

$$\begin{aligned}\mathcal{P}(\hat{M}) \;&=\; \sum_{a\in\mathcal{A}}\sum_{k\in\Omega} w_a(k)\,\mathbf{1}[k\in\Omega_a] \;=\; \sum_{a\in\mathcal{A}}\sum_{k\in\Omega} w_{\max}(k)\,\mathbf{1}[k\in\Omega_a] \\ &=\; \sum_{k\in\Omega} w_{\max}(k)\left(\sum_{a\in\mathcal{A}} \mathbf{1}[k\in\Omega_a]\right) \;=\; \sum_{k\in\Omega} w_{\max}(k)\,. \end{aligned} \tag{IV.19}$$

It follows that

$$\mathcal{P}(M) \;\leq\; \sum_{k \in \Omega} w_{\max}(k) \;=\; \mathcal{P}(\hat{M}) \;=\; \mathcal{P}_{\max} \,. \tag{IV.20}$$

Finally, we define

$$\Lambda \;:=\; \sum_{k \in \Omega} w_{\max}(k) \, |f_k\rangle\langle f_k| \,. \tag{IV.21}$$

Then obviously $\Lambda \geq W_a$, for all $a \in \mathcal{A}$, and $\mathrm{Tr}(\Lambda) = \sum_{k \in \Omega} w_{\max}(k) = \mathcal{P}_{\max}$. Thus $\widetilde{\mathcal{P}}_{\max} = \mathcal{P}_{\max}$, as asserted in Theorem IV.3 (iii), below.

We conclude that if the density matrices ρ_a mutually commute, then the average probability of making a correct prediction is maximized by an *orthogonal* resolution of the identity.

In the above example, the assumption that the density matrices $\rho_1, \rho_2, \ldots, \rho_d$ are mutually commuting is of key importance for the explicit determination of the optimal resolution $\hat{M}$ of the identity which maximizes the average probability $\mathcal{P}(M)$ of making a correct prediction property.

There is a second special situation in which the optimal resolution of the identity can be determined, namely, for $d = 2$, as is demonstrated in Theorem **??**. Before going into this we recall a few facts from matrix analysis. First we note that if $A, B \in \mathcal{SA}(\mathcal{H})$ with $A, B \geq 0$ then $A^{1/2} B A^{1/2} \geq 0$ and hence

$$\mathrm{Tr}(AB) \;=\; \mathrm{Tr}\big(A^{1/2} B A^{1/2}\big) \;\geq\; 0 \,. \tag{IV.22}$$

If furthermore $B \leq C$ then $A^{1/2}(C - B)A^{1/2} \geq 0$ and (IV.22) implies that

$$\mathrm{Tr}(AB) \;=\; \mathrm{Tr}\big(A^{1/2} B A^{1/2}\big) \;\leq\; \mathrm{Tr}\big(A^{1/2} C A^{1/2}\big) \;=\; \mathrm{Tr}(AC) \,. \tag{IV.23}$$

Eqs. (IV.22) can alternatively be shown by using the spectral theorem for $A = \sum_{j=1}^{D} \lambda_j |f_j\rangle\langle f_j|$, where $\lambda_j \geq 0$ are the eigenvalues and f_j the orthonormal eigenvectors of A, respectively.

We also note that the *positive part* $(\cdot)_+ \in C(\mathbb{R}; \mathbb{R}_0^+)$ of a real number is defined by

$$\forall\, \lambda \in \mathbb{R} : \quad (\lambda)_+ \;:=\; \max\{\lambda,\, 0\} \;=\; \lambda \, \mathbf{1}[\lambda > 0] \;=\; \frac{1}{2}|\lambda| + \frac{1}{2}\lambda \,. \tag{IV.24}$$

Theorem IV.2. *Let $U, V \in \mathcal{SA}(\mathcal{H})$ be two positive operators, and define*

$$\widetilde{\mathcal{P}}_{\min} \;:=\; \inf \Big\{ \mathrm{Tr}(\Lambda) \;\Big|\; \Lambda \in \mathcal{SA}(\mathcal{H}) \,,\; \Lambda \geq U \,,\; \Lambda \geq V \;\Big\} . \tag{IV.25}$$

Then

$$\Lambda_0 \;:=\; \frac{1}{2}(U + V) \;+\; \frac{1}{2}|U - V| \;=\; V \;+\; (U - V)_+ \;=\; U \;+\; (V - U)_+ \tag{IV.26}$$

defined by the functional calculus from Definition II.3, is the unique operator $\Lambda_0 \in \mathcal{SA}(\mathcal{H})$ obeying $\Lambda_0 \geq U$ and $\Lambda_0 \geq V$, such that $\widetilde{\mathcal{P}}_{\min} = \mathrm{Tr}(\Lambda_0)$. Moreover,

$$\widetilde{\mathcal{P}}_{\min} \;=\; \mathcal{P}_{\max} \;=\; \sup \Big\{ \mathrm{Tr}[UM + V(\mathbf{1} - M)] \;\Big|\; M \in \mathcal{SA}(\mathcal{H}) \,,\; 0 \leq M \leq \mathbf{1} \Big\} . \tag{IV.27}$$

Proof. Define Λ_0 by (IV.26) and note that $\Lambda_0 = V + (U-V)_+ \geq V$ and $\Lambda_0 = U + (V-U)_+ \geq U$. We introduce the orthogonal projections

$$P_+ \ := \ \mathbf{1}[U - V \geq 0] \quad \text{and} \quad P_- \ := \ P_+^\perp \ = \mathbf{1}[U - V < 0] \ = \ \mathbf{1}[V - U > 0] \tag{IV.28}$$

and oberve that

$$P_+ \, \Lambda_0 \, P_+ \ = \ P_+ \, U \, P_+ \quad \text{and} \quad P_- \, \Lambda_0 \, P_- \ = \ P_- \, V \, P_- \, , \tag{IV.29}$$

which implies that

$$\mathcal{F}(U, V) \ \leq \ \mathrm{Tr}(\Lambda_0) \ = \ \mathrm{Tr}(P_+ \, U \, P_+) \ + \ \mathrm{Tr}(P_- \, V \, P_-) \, . \tag{IV.30}$$

Next suppose that $\Gamma \in \mathcal{SA}(\mathcal{H})$ obeys $\Gamma \geq U$ and $\Gamma \geq W$ and minizimes $\mathrm{Tr}(\Gamma)$. Then

$$\begin{aligned} \mathcal{F}(U, V) \ &= \mathrm{Tr}(\Gamma) \ = \ \mathrm{Tr}(P_+ \, \Gamma \, P_+) \ + \ \mathrm{Tr}(P_- \, \Gamma \, P_-) \\ &= \mathrm{Tr}(\Lambda_0) \ + \ \mathrm{Tr}[P_+ \, (\Gamma - U) \, P_+] \ + \ \mathrm{Tr}[P_- \, (\Gamma - V) \, P_-] \, , \end{aligned} \tag{IV.31}$$

which implies that Λ_0 is a minimizer, $\mathcal{F}(U, V) = \mathrm{Tr}(\Lambda_0)$, indeed. Furthermore, it follows from (IV.31) and (IV.29) that

$$P_+ \, \Gamma \, P_+ \ = \ P_+ \, \Lambda_0 \, P_+ \quad \text{and} \quad P_- \, \Gamma \, P_- \ = \ P_- \, \Lambda_0 \, P_- \, . \tag{IV.32}$$

Now assume that $\Theta := \Gamma - \Lambda_0 \neq 0$. Then $\Theta = P_+ \Theta P_- + P_- \Theta P_+$ and

$$\Gamma - U \ = \ \Lambda_0 - U + \Theta \ = \ (V - U)_+ + \Theta \ = \ P_-(V - U)P_- + P_+ \Theta P_- + P_- \Theta P_+ \, . \tag{IV.33}$$

Since $\Theta \neq 0$, there exist $\varphi_\pm = P_\pm \varphi_\pm \neq 0$ such that $\langle \varphi_- | \Theta \varphi_+ \rangle \neq 0$. For any $\varepsilon > 0$ and $|\sigma| = 1$, we define $\psi_{\varepsilon,\sigma} := \sigma \varphi_+ + \varepsilon \varphi_-$ and observe that, thanks to (IV.33), we have

$$\langle \psi_{\varepsilon,\sigma} | (\Gamma - U) \psi_{\varepsilon,\sigma} \rangle \ = \ 2\varepsilon \, \mathrm{Re}\big\{ \sigma \, \langle \varphi_- | \Theta \varphi_+ \rangle \big\} \ + \ \varepsilon^2 \, \langle \varphi_- | (V - U) \varphi_- \rangle \, . \tag{IV.34}$$

Choosing σ such that $\sigma \, \langle \varphi_- | \Theta \varphi_+ \rangle = -|\langle \varphi_- | \Theta \varphi_+ \rangle| < 0$, we obtain

$$\langle \psi_{\varepsilon,\sigma} | (\Gamma - U) \psi_{\varepsilon,\sigma} \rangle \ < \ 0 \, , \tag{IV.35}$$

for $\varepsilon > 0$ sufficiently small. This contradicts $\Gamma \geq U$. It follows that $\Theta = 0$ and hence the uniqueness of the minimizer Λ_0.

Finally, if $0 \leq M \leq \mathbf{1}$ then

$$\begin{aligned} &\mathrm{Tr}\{UM + V(\mathbf{1} - M)\} \\ &\qquad = \mathrm{Tr}\{V\} + \mathrm{Tr}\{(U - V)M\} \ = \ \mathrm{Tr}\{V\} + \mathrm{Tr}\{M^{1/2}(U - V)M^{1/2}\} \\ &\qquad \leq \mathrm{Tr}\{V\} + \mathrm{Tr}\{M^{1/2}(U - V)_+ M^{1/2}\} \ = \ \mathrm{Tr}\{V\} + \mathrm{Tr}\{(U - V)_+^{1/2} M (U - V)_+^{1/2}\} \\ &\qquad \leq \mathrm{Tr}\{V\} + \mathrm{Tr}\{(U - V)_+\} \ = \ \widetilde{\mathcal{P}}_{\min} \, , \end{aligned} \tag{IV.36}$$

which implies that $\mathcal{P}_{\max} \leq \widetilde{\mathcal{P}}_{\min}$. Conversely, if $\hat{M} := \mathbf{1}[U - V \geq 0]$ then

$$\begin{aligned} \mathrm{Tr}\{U\hat{M} + V(\mathbf{1} - \hat{M})\} &= \mathrm{Tr}\{V + (U-V)\hat{M}\} \;=\; \mathrm{Tr}\{V + (U-V)_+\} \\ &= \mathrm{Tr}\{\Lambda_0\} \;=\; \widetilde{\mathcal{P}}_{\min}\,, \end{aligned} \tag{IV.37}$$

hence $\widetilde{\mathcal{P}}_{\min} \leq \mathcal{P}_{\max}$. □

Remarks and Examples. Let $\mathcal{A} = \{0, 1\}$ and again $\Omega = \mathbb{Z}_1^N = \{1, 2, \ldots, N\}$ such that $\mathcal{H} = \ell^2(\Omega) \cong \mathbb{C}^N$ is the Hilbert space of states. Suppose that we are given two density matrices $\rho_0, \rho_1 \in \mathcal{DM}(\mathcal{H})$ that are chosen with probability $\pi_0 \in (0,1)$ and $\pi_1 = 1 - \pi_0$, respectively. We introduce $W_0 := \pi_0\rho_0 \geq 0$ and $W_1 := \pi_1\rho_1 \geq 0$, as before.

A resolution $M = \{M_0, M_1\} \subseteq \mathcal{SA}(\mathcal{H})$ of the identity is necessarily of the form $M_1 = \mathbf{1} - M_0$ and hence fully determined by the choice of $0 \leq M_0 \leq \mathbf{1}$. Given M_0, and hence M, we observe that

$$\mathcal{P}(M) = \mathrm{Tr}[W_0 M_0] + \mathrm{Tr}[W_1(\mathbf{1} - M_0)] = \mathrm{Tr}[W_1] + \mathrm{Tr}[(W_0 - W_1)M_0]\,. \tag{IV.38}$$

Since $W_0 - W_1 \in \mathcal{SA}(\mathcal{H})$, there is an ONB $\{f_k\}_{k\in\Omega} \subseteq \mathcal{H}$ of eigenvectors of $W_0 - W_1$ with corresponding eigenvalues $\lambda_k \in \mathbb{R}$ such that

$$W_0 - W_1 = \sum_{k\in\Omega} \lambda_k\, |f_k\rangle\langle f_k| \tag{IV.39}$$

and, therefore,

$$\mathrm{Tr}[(W_0 - W_1)M_0] = \sum_{k\in\Omega} \lambda_k\, \langle f_k|\, M_0 f_k\rangle = \sum_{k\in\Omega} (\lambda_k)_+\,, \tag{IV.40}$$

using that $\langle f_k|M_0 f_k\rangle \in [0,1]$, where the *positive part* $(\cdot)_+ : \mathbb{R} \to \mathbb{R}_0^+$ of a real number is defined by

$$\forall\, \lambda \in \mathbb{R} : \quad (\lambda)_+ := \max\{\lambda, 0\} = \lambda\, \mathbf{1}[\lambda > 0] = \frac{1}{2}|\lambda| + \frac{1}{2}\lambda\,. \tag{IV.41}$$

By the functional calculus as in Definition II.3, we have that

$$\mathrm{Tr}[(W_0 - W_1)M_0] \leq \mathrm{Tr}[(W_0 - W_1)_+]\,, \tag{IV.42}$$

for any $0 \leq M_0 \leq \mathbf{1}$, where

$$(W_0 - W_1)_+ = \sum_{k\in\Omega} (\lambda_k)_+\, |f_k\rangle\langle f_k|\,. \tag{IV.43}$$

Again by the functional calculus as in Definition II.3, we define

$$\hat{M}_0 := \mathbf{1}[W_0 - W_1 > 0] = \sum_{k\in\Omega} \mathbf{1}[\lambda_k > 0]\, |f_k\rangle\langle f_k|\,. \tag{IV.44}$$

Then $0 \leq \hat{M}_0 \leq \mathbf{1}$ and

$$\mathrm{Tr}[(W_0 - W_1)\hat{M}_0] \;=\; \mathrm{Tr}[(W_0 - W_1)_+]\,, \tag{IV.45}$$

which implies that $\hat{M} = \{\hat{M}_0, \mathbf{1} - \hat{M}_0\} \subseteq \mathcal{SA}(\mathcal{H})$ is a (sharp) resolution of the identity which maximizes the average probability of making a correct prediction,

$$\begin{aligned}
\mathcal{P}(\hat{M}) &= \mathrm{Tr}[W_1 + (W_0 - W_1)_+] \;=\; \mathrm{Tr}\big(W_1 + \tfrac{1}{2}|W_0 - W_1| + \tfrac{1}{2}(W_0 - W_1)\big) \\
&= \frac{1}{2}\mathrm{Tr}\big(W_0 + W_1\big) \;+\; \frac{1}{2}\mathrm{Tr}\big(|W_0 - W_1|\big) \\
&= \frac{1}{2}\big[\pi_0\,\mathrm{Tr}(\rho_0) \;+\; \pi_1\,\mathrm{Tr}(\rho_1)\big] \;+\; \frac{1}{2}\mathrm{Tr}\big(|\pi_0\rho_0 - \pi_1\rho_1|\big) \\
&= \frac{1}{2} \;+\; \frac{1}{2}\|\pi_0\rho_0 - \pi_1\rho_1\|_{\mathcal{L}^1(\mathcal{H})}\,.
\end{aligned} \tag{IV.46}$$

Now, we generalize Theorem IV.2 from $d = 2$ to general $d \in \mathbb{N}$. In this general case, the characterization of the optimal resolution of identity is, however, somewhat implicit.

Theorem IV.3. *Let $\big(\mathcal{H}, \langle\cdot|\cdot\rangle\big)$ be a Hilbert space and $\mathcal{A}$ a finite set with at least two elements. Further suppose that $\{\rho_a\}_{a\in\mathcal{A}} \in \mathcal{DM}(\mathcal{H})$ is a finite collection of density matrices on $\mathcal{H}$ and $\pi : \mathcal{A} \to (0,1)$ is a probability distribution, such that π_b is the probability that a random density matrix $\rho \in \{\rho_a\}_{a\in\mathcal{A}}$ assumes the value ρ_b and define $W_a := \pi_a\rho_a$, for all $a \in \mathcal{A}$, and*

$$\widetilde{\mathcal{P}}_{\min} \;:=\; \inf\Big\{\mathrm{Tr}(\Lambda)\;\Big|\;\forall\, a \in \mathcal{A} :\; \Lambda \geq W_a\Big\}. \tag{IV.47}$$

- *(i) If $\hat{M} = \{\hat{M}_a\}_{a\in\mathcal{A}} \in \mathfrak{M}_{\mathcal{A}}(\mathcal{H})$ is a resolution of the identity with maximal average probability of making a correct decision, $\mathcal{P}(\hat{M}) = \mathcal{P}_{\max}$. Then there exists $\Lambda = \Lambda^* \in \mathcal{B}(\mathcal{H})$ such that*

$$\forall\, a \in \mathcal{A} : \qquad \big(\Lambda - W_a\big)\hat{M}_a \;=\; 0\,, \tag{IV.48}$$

$$\forall\, a \in \mathcal{A} : \qquad \Lambda \;\geq\; W_a\,. \tag{IV.49}$$

- *(ii) Conversely, if a resolution of the identity $\hat{M} = \{\hat{M}_a\}_{a\in\mathcal{A}} \in \mathfrak{M}_{\mathcal{A}}(\mathcal{H})$ and an operator $\Lambda = \Lambda^* \in \mathcal{B}(\mathcal{H})$ fulfill* (IV.48) *and* (IV.49)*, then $\mathcal{P}(\hat{M}) = \mathcal{P}_{\max}$.*
- *(iii) There is a unique $\widehat{\Lambda} \in \mathcal{SA}(\mathcal{H})$ obeying $\widehat{\Lambda} \geq W_a$, for all $a \in \mathcal{A}$, such that*

$$\mathcal{P}_{\max} \;=\; \widetilde{\mathcal{P}}_{\min} \;=\; \mathrm{Tr}(\widehat{\Lambda})\,. \tag{IV.50}$$

Proof. We first introduce

$$\mathfrak{L}(W) \;:=\Big\{\Lambda \in \mathcal{SA}(\mathcal{H})\;\Big|\;\forall\, a \in \mathcal{A} : \quad \Lambda \geq W_a\Big\} \tag{IV.51}$$

and define

$$\mathcal{F}(M,\Lambda) := \sum_{a\in\mathcal{A}} \mathrm{Tr}\big[W_a\, M_a\big] \;-\; \mathrm{Tr}\Big[\Lambda\Big(\sum_{a\in\mathcal{A}} M_a - \mathbf{1}\Big)\Big] \tag{IV.52}$$
$$= \mathrm{Tr}[\Lambda] \;-\; \sum_{a\in\mathcal{A}} \mathrm{Tr}\big[(\Lambda - W_a)\, M_a\big]\,,$$

for $M \in \mathcal{SA}(\mathcal{H})^{\mathcal{A}}$ and $\Lambda \in \mathcal{SA}(\mathcal{H})$. Note that, for all $\Lambda \in \mathfrak{L}(W)$,

$$\widetilde{\mathcal{P}}(\Lambda) \;:=\; \sup_{\chi\in\mathcal{SA}(\mathcal{H})^{\mathcal{A}}} \mathcal{F}(\chi^2,\Lambda) \;=\; \max_{\chi\in\mathcal{SA}(\mathcal{H})^{\mathcal{A}}} \mathcal{F}(\chi^2,\Lambda) \;=\; \mathcal{F}(0,\Lambda) \;=\; \mathrm{Tr}[\Lambda]\,, \tag{IV.53}$$

writing $(\chi^2)_a := \chi_a^2$. Conversely, for all $\Lambda \in \mathcal{SA}(\mathcal{H}) \setminus \mathfrak{L}(W)$, there is an $\tilde{a} \in \mathcal{A}$ and $\varphi \in \mathcal{H} \setminus \{0\}$ such that $W_{\tilde{a}} - \Lambda \geq |\varphi\rangle\langle\varphi|$. Then, choosing $\chi_a = 0$ except $\chi_{\tilde{a}}$, which is chosen as $\chi_{\tilde{a}} := \mu|\varphi\rangle\langle\varphi|$, we obtain that

$$\widetilde{\mathcal{P}}(\Lambda) \;\geq\; \sup_{\mu\in\mathbb{R}} \big\{\mu^2\, \|\varphi\|^4\big\} \;=\; \infty\,. \tag{IV.54}$$

So, if we define $\widetilde{\mathcal{P}} : \mathcal{SA}(\mathcal{H}) \to \mathbb{R} \cup \{\infty\}$, with $\infty > x$, for any $x \in \mathbb{R}$, it follows that

$$\widetilde{\mathcal{P}}_{\min} \;=\; \min_{\Lambda\in\mathcal{SA}(\mathcal{H})} \{\widetilde{\mathcal{P}}(\Lambda)\} \;=\; \min_{\Lambda\in\mathfrak{L}(W)} \{\widetilde{\mathcal{P}}(\Lambda)\}\,. \tag{IV.55}$$

(i): Let $\hat{\chi} \in \mathcal{SA}(\mathcal{H})^{\mathcal{A}}$ be such that $\hat{M} = \hat{\chi}^2 \in \mathfrak{M}_{\mathcal{A}}(\mathcal{H})$ is a maximizer of $\mathcal{P}$, i.e.,

$$\mathcal{P}(\hat{\chi}^2) \;=\; \max_{M\in\mathfrak{M}_{\mathcal{A}}(\mathcal{H})} \{\mathcal{P}(M)\} \tag{IV.56}$$
$$=\; \max\Big\{\mathcal{P}(M) \;\Big|\; M = (\chi_a^2)_{a\in\mathcal{A}}\,,\; \forall\, a \in \mathcal{A} : \chi_a \in \mathcal{SA}(\mathcal{H})\,,\; \sum_{a\in\mathcal{A}} \chi_a^2 = \mathbf{1}\Big\}\,.$$

The theory of extrema of multivariate functions under constraints implies that there is a family of Lagrange mutlipliers which we can arrange as real and imaginary parts of the matrix entries of a self-adjoint matrix $\Lambda \in \mathcal{SA}(\mathcal{H})$ such that $\mathcal{SA}(\mathcal{H})^{\mathcal{A}} \ni \chi \mapsto \mathcal{F}(\chi^2,\Lambda) \in \mathbb{R}$ is stationary at $\hat{\chi}$. Moreover, by results from convex analysis we may even assume that $\hat{\chi}$ is a maximizer of $\mathcal{SA}(\mathcal{H})^{\mathcal{A}} \ni \chi \mapsto \mathcal{F}(\chi^2,\Lambda) \in \mathbb{R}$. Then, for all $\varepsilon > 0$ and all $\theta = (\theta_a)_{a\in\mathcal{A}} \in \mathcal{SA}(\mathcal{H})^{\mathcal{A}}$,

$$0 \;\leq \mathcal{F}\big[\hat{\chi}^2,\Lambda\big] \;-\; \mathcal{F}\big[(\hat{\chi}+\varepsilon\theta)^2,\Lambda\big] \tag{IV.57}$$
$$= \varepsilon \sum_{a\in\mathcal{A}} \mathrm{Tr}\Big\{\big[(\Lambda - W_a)\hat{\chi}_a + \hat{\chi}_a(\Lambda - W_a)\big]\theta_a\Big\} \;+\; \varepsilon^2 \sum_{a\in\mathcal{A}} \mathrm{Tr}\big\{\theta_a(\Lambda - W_a)\theta_a\big\}\,.$$

Since θ can be chosen arbitrarily, taking the limit $\varepsilon \to$ yields

$$\forall\, a \in \mathcal{A} : \qquad (\Lambda - W_a)\hat{\chi}_a + \hat{\chi}_a(\Lambda - W_a) \;=\; 0\,. \tag{IV.58}$$

From this we obtain for all $a \in \mathcal{A}$ that $(\Lambda - W_a)\hat{\chi}_a = -\hat{\chi}_a(\Lambda - W_a)$, which implies $(\Lambda - W_a)^2\hat{\chi}_a = \hat{\chi}_a(\Lambda - W_a)^2$ and, hence, for all $r > 0$ that

$$\big[(\Lambda - W_a)^2 + r^2\big]^{-1}\,\hat{\chi}_a \;=\; \hat{\chi}_a\,\big[(\Lambda - W_a)^2 + r^2\big]^{-1}. \tag{IV.59}$$

Using $\sqrt{A} = \frac{A}{\pi}\int_0^\infty (A + r^2)^{-1}\,dr$, we obtain

$$|\Lambda - W_a|\,\hat{\chi}_a \;=\; \sqrt{(\Lambda - W_a)^2}\,\hat{\chi}_a \;=\; \hat{\chi}_a\,\sqrt{(\Lambda - W_a)^2} \;=\; \hat{\chi}_a\,|\Lambda - W_a|\,, \tag{IV.60}$$

and finally

$$\begin{aligned}(\Lambda - W_a)_\pm\,\hat{\chi}_a \;&= \tfrac{1}{2}|\Lambda - W_a|\,\hat{\chi}_a \;\pm\; \tfrac{1}{2}(\Lambda - W_a)\,\hat{\chi}_a \\ &= \hat{\chi}_a\,\tfrac{1}{2}|\Lambda - W_a| \;\mp\; \tfrac{1}{2}\hat{\chi}_a\,(\Lambda - W_a) \;=\; \hat{\chi}_a\,(\Lambda - W_a)_\mp\,.\end{aligned} \tag{IV.61}$$

On the other hand, inserting (IV.58) into (IV.57), we further obtain that

$$0 \;\leq\; \varepsilon^2 \sum_{a\in\mathcal{A}} \mathrm{Tr}\big\{\theta_a(\Lambda - W_a)\theta_a\big\}\,. \tag{IV.62}$$

Since $\theta_a \in \mathcal{SA}(\mathcal{H})$ is arbitrary, this implies that $\Lambda \geq W_a$, for all $a \in \mathcal{A}$, i.e., that

$$\Lambda \;\in\; \mathfrak{L}(W)\,. \tag{IV.63}$$

Moreover, $\Lambda \geq W_a$ is equivalent to $(\Lambda - W_a)_- = 0$, which together with (IV.61) yields

$$\forall\, a \in \mathcal{A}: \qquad (\Lambda - W_a)\,M_a \;=\; (\Lambda - W_a)_+\,M_a \;=\; \hat{\chi}_a\,(\Lambda - W_a)_-\,\hat{\chi}_a \;=\; 0\,. \tag{IV.64}$$

This completes the proof of *(i)*.

(ii): Let $\Lambda \in \mathfrak{L}(W)$ and $M = \{M_a\}_{a\in\mathcal{A}} \in \mathfrak{M}_{\mathcal{A}}(\mathcal{H})$ be a resolution of the identity. Then

$$\mathcal{P}(M) \;=\; \sum_{a\in\mathcal{A}} \mathrm{Tr}[W_a\,M_a] \;=\; \mathrm{Tr}(\Lambda) \;-\; \sum_{a\in\mathcal{A}} \mathrm{Tr}[(\Lambda - W_a)\,M_a] \;\leq\; \mathrm{Tr}(\Lambda) \;=\; \widetilde{\mathcal{P}}(\Lambda)\,. \tag{IV.65}$$

It follows that

$$\mathcal{P}_{\max} \;=\; \max_{M\in\mathfrak{M}_{\mathcal{A}}(\mathcal{H})} \mathcal{P}(\hat{M}) \;\leq\; \min_{\Lambda\in\mathfrak{L}(W)} \widetilde{\mathcal{P}}(\Lambda) \;=\; \widetilde{\mathcal{P}}_{\min}\,. \tag{IV.66}$$

If $\hat{M} = \{\hat{M}_a\}_{a\in\mathcal{A}} \in \mathfrak{M}_{\mathcal{A}}(\mathcal{H})$ additionally fulfills (IV.48) then

$$\mathcal{P}(\hat{M}) \;=\; \mathrm{Tr}(\Lambda) \;-\; \sum_{a\in\mathcal{A}} \mathrm{Tr}[(\Lambda - W_a)\,M_a] \;=\; \mathrm{Tr}(\Lambda) \;=\; \widetilde{\mathcal{P}}(\Lambda)\,. \tag{IV.67}$$

and hence $\mathcal{P}(\hat{M}) = \mathcal{P}_{\max}$ and $\widetilde{\mathcal{P}}(\Lambda) = \widetilde{\mathcal{P}}_{\min}$.

(iii): is obvious from what has been proven so far except the uniqueness of the minimizer $\widehat{\Lambda} \in \mathfrak{L}(W)$ of $\widetilde{\mathcal{P}}_(\Lambda)$, which we omit here. □

Remarks and Examples. We exemplify Theorem IV.3 on a single qubit, i.e., $\mathcal{H} = \mathbb{C}^2$ and we assume that $\mathcal{A} = \{1, 2, 3\}$. We are given $\pi_1, \pi_2, \pi_3 \in (0, 1)$ such that $\pi_1 + \pi_2 + \pi_3 = 1$ and $\vec{v}_1, \vec{v}_2, \vec{v}_3 \in \overline{B(0,1)} \subseteq \mathbb{R}^3$ that determine three density matrices $\rho_1, \rho_2, \rho_3 \in \mathcal{DM}(\mathcal{H})$ and operators $W_a = \pi_a \rho_a$ by

$$\rho_a \; = \; \frac{1}{2}\Big(\mathbf{1} \, + \, \vec{v}_a \cdot \vec{\sigma}\Big) , \qquad W_a \; = \; \frac{\pi_a}{2}\Big(\mathbf{1} \, + \, \vec{v}_a \cdot \vec{\sigma}\Big) . \tag{IV.68}$$

We assume that $\Lambda \in \mathcal{SA}(\mathcal{H})$ is positive and hence determined by $r > 0$ and $\vec{z} \in \overline{B(0,r)}$ as

$$\Lambda \; = \; \frac{r}{2}\mathbf{1} \, + \, \vec{z} \cdot \vec{\sigma} . \tag{IV.69}$$

We observe that, for $a \in \mathcal{A}$,

$$\Lambda - W_a \; = \; \frac{r - \pi_a}{2}\mathbf{1} \, + \, \left(\frac{\vec{z} - \pi_a \vec{v}_a}{2}\right) \cdot \vec{\sigma} , \tag{IV.70}$$

so, if $\Lambda - W_a \geq 0$ then necessarily $r > \pi_a$ and $r - \pi_a \geq |\vec{z} - \pi_a \vec{v}_a|$. The latter condition is equivalent to

$$(r - \pi_a)^2 \; \geq \; |\vec{z}|^2 + \pi_a^2 |\vec{v}_a|^2 - 2\pi_a \vec{z} \cdot \vec{v}_a . \tag{IV.71}$$

Now we concretely choose $\pi_1 = \pi_2 = \pi_3 = \frac{1}{3}$ and

$$\vec{v}_a \; := \; \begin{pmatrix} \sin(\frac{4\pi}{3}a) \\ 0 \\ \cos(\frac{4\pi}{3}a) \end{pmatrix} , \; \text{ i.e., } \vec{v}_1 \; := \; \begin{pmatrix} \frac{1}{2}\sqrt{3} \\ 0 \\ -\frac{1}{2} \end{pmatrix} , \; \vec{v}_2 \; := \; \begin{pmatrix} -\frac{1}{2}\sqrt{3} \\ 0 \\ -\frac{1}{2} \end{pmatrix} , \; \vec{v}_3 \; := \; \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} , \tag{IV.72}$$

which implies that $|\vec{v}_1| = |\vec{v}_2| = |\vec{v}_3| = 1$ and simplifies the three conditions (IV.71) to a single one,

$$\big(r - \tfrac{1}{3}\big)^2 \; \geq \; \tfrac{1}{9} + \max_{a \in \mathcal{A}} \Big\{ |\vec{z}|^2 - \tfrac{2}{3}\vec{z} \cdot \vec{v}_a \Big\} . \tag{IV.73}$$

Writing $\vec{z} = (z_1, z_2, z_3)^t$, we observe that

$$\begin{aligned} &\max_{a \in \mathcal{A}} \Big\{ |\vec{z}|^2 - \tfrac{2}{3}\vec{z} \cdot \vec{v}_a \Big\} \\ &= \max \Big\{ z_1^2 + z_2^2 + z_3^2 - \tfrac{1}{\sqrt{3}} z_1 + \tfrac{1}{3} z_3 \, , \;\; z_1^2 + z_2^2 + z_3^2 + \tfrac{1}{\sqrt{3}} z_1 + \tfrac{1}{3} z_3 \, , \\ &\qquad\qquad z_1^2 + z_2^2 + z_3^2 - \tfrac{2}{3} z_3 \Big\} \\ &= \max \Big\{ z_1^2 + z_2^2 + z_3^2 + \tfrac{1}{\sqrt{3}} |z_1| + \tfrac{1}{3} z_3 \, , \;\; z_1^2 + z_2^2 + z_3^2 - \tfrac{2}{3} z_3 \Big\} \\ &\geq z_1^2 + z_2^2 + z_3^2 + \tfrac{1}{3} |z_3| . \end{aligned} \tag{IV.74}$$

This, however, implies that $\vec{z} = \vec{0}$ is the best possible choice for $\vec{z}$ because it imposes the least constraint on r in (IV.73). In turn, if $\vec{z} = \vec{0}$ then the smallest $r > \frac{1}{3}$ fulfilling (IV.73) is $r = \frac{2}{3}$. As $\mathrm{Tr}(\Lambda) = r$, it follows that the optimal choice for Λ is

$$\Lambda \; = \; \frac{1}{3}\mathbf{1} \qquad \text{and} \qquad \widetilde{\mathcal{P}}_{\min} \; = \; \mathrm{Tr}(\Lambda) \; = \; \frac{2}{3} . \tag{IV.75}$$