Part IV

Quantum Information Theory

Chapter 8

Measures of Quantum Information

8.1 Quantum Min-Entropy

We define the quantum counterpart of the classical min-entropy (Definition A.4). By convention, here and throughout the rest of the notes, log denotes the *binary* logarithm, i.e., the logarithm to base 2.

Definition 8.1. *For a given* $\rho_A \in \mathcal{D}(A)$ *the* **min-entropy** *of* A *is*

$$\mathrm{H}_\infty(A) := \mathrm{H}_\infty(\rho_A) := -\log \lambda_{\max}(\rho_A) = -\log \|\rho_A\|_\infty \,.$$

Obviously, if ρ_X is classical, then the definition coincides with the classical notion. Also, we see that for any $\rho_A \in \mathcal{D}(A)$, its min-entropy is bounded by $0 \leq \mathrm{H}_\infty(A) \leq \log \dim(\mathcal{H}_A)$, as for the classical counterpart. However, in certain other aspects, the quantum version behaves very differently. For instance, if AB is an EPR pair, i.e. $\rho_{AB} = |\Phi\rangle\langle\Phi|$ with $|\Phi\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle + |1\rangle|1\rangle\big)$, then $\rho_A = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ and thus

$$\mathrm{H}_\infty(A) = 1 > 0 = \mathrm{H}_\infty(AB)\,,$$

meaning that the entropy can decrease when considering a larger system. In other words, the quantum version of H_∞ violates **monotonicity** (see Lemma A.4). This is an artifact of entanglement.

How to define the quantum version of the *conditional* min-entropy is way less obvious. We start with the following auxiliary definition.

Definition 8.2. *Let* $\rho_{AE} \in \mathcal{D}(AE)$ *and* $\sigma_E \in \mathcal{D}(E)$*. Then, the* **min-entropy** *of* ρ_{AE} **relative to** σ_E *is given by*

$$\mathrm{H}_\infty(\rho_{AE}|\sigma_E) := -\log \min\{\lambda > 0 \,|\, \lambda \cdot \mathbb{I}_A \otimes \sigma_E \geq \rho_{AE}\}\,.$$

with the understanding that $\mathrm{H}_\infty(\rho_{AE}|\sigma_E) = -\infty$ *if no such* λ *exists.*

Remark 8.1. If $\mathrm{supp}(\rho_{AE}) \not\subseteq \mathrm{supp}(\mathbb{I}_A \otimes \sigma_E)$ then there is no λ satisfying the inequality. Indeed, if $|\Omega\rangle \in \ker(\mathbb{I}_A \otimes \sigma_E)$ but not in $\ker(\rho_{AE})$ then $\lambda \cdot \langle\Omega|(\mathbb{I}_A \otimes \sigma_E)|\Omega\rangle = 0 < \langle\Omega|\rho_{AE}|\Omega\rangle$ for any choice of λ (exploiting Remark 0.3). Below, we show that the necessary condition $\mathrm{supp}(\rho_{AE}) \subseteq \mathrm{supp}(\mathbb{I}_A \otimes \sigma_E)$ for $\mathrm{H}_\infty(\rho_{AE}|\sigma_E)$ to be finite is equivalent to $\mathrm{supp}(\rho_E) \subseteq \mathrm{supp}(\sigma_E)$ (Corollary 8.2), and that this condition is also sufficient (Lemma 8.3).

Lemma 8.1. *Let* $0 \leq R_{AE} \in \mathcal{L}(\mathcal{H}_{AE})$*,* $R_E = \mathrm{tr}_A(R_{AE})$*, and* $|\varphi\rangle \in \mathcal{H}_E$*. Then:*

$$|\varphi\rangle \in \ker(R_E) \iff |\psi\rangle|\varphi\rangle \in \ker(R_{AE}) \;\forall\, |\psi\rangle \in \mathcal{H}_A\,.$$

Furthermore, $\ker(\mathbb{I}_A \otimes R_E) = \mathcal{H}_A \otimes \ker(R_E) \subseteq \ker(R_{AE})$.

Proof. Let $\{|i\rangle\}_{i\in I}$ be an arbitrary orthonormal basis of $\mathcal{H}_A$. The equivalence claim then follows from the observation that

$$\begin{aligned}\sum_i \langle i|\langle\varphi|R_{AE}|i\rangle|\varphi\rangle &= \sum_i \operatorname{tr}\big(R_{AE}(|i\rangle\langle i|\otimes|\varphi\rangle\langle\varphi|)\big)\\ &= \operatorname{tr}\big(R_{AE}(\mathbb{I}\otimes|\varphi\rangle\langle\varphi|)\big) = \operatorname{tr}(R_E|\varphi\rangle\langle\varphi|) = \langle\varphi|R_E|\varphi\rangle\,,\end{aligned}$$

together with Remark 0.3 and the positivity of both R_{AE} and R_E.

Regarding the second claim, we first note that the subset-claim follows directly from the proven $\Rightarrow$-implication. For the equality, consider $|\Phi\rangle \in \mathcal{H}_{AE}$, written as $|\Phi\rangle = \sum_i \alpha_i|i\rangle|\varphi_i\rangle$, and note that

$$\langle\Phi|(\mathbb{I}_A\otimes R_E)|\Phi\rangle = \sum_i |\alpha_i|^2\langle\varphi_i|R_E|\varphi_i\rangle\,.$$

Thus, again exploiting Remark 0.3,

$$|\Phi\rangle\in\ker(\mathbb{I}_A\otimes R_E) \iff |\varphi_i\rangle\in\ker(R_E)\ \forall\, i \text{ with } \alpha_i\neq 0 \iff |\Phi\rangle\in\mathcal{H}_A\otimes\ker(R_E)\,,$$

which then completes the proof. □

Corollary 8.2. *For any* $0\le R_{AE}\in\mathcal{L}(\mathcal{H}_A\otimes\mathcal{H}_E)$ *and* $0\le L_E\in\mathcal{L}(H_E)$*:*

$$\operatorname{supp}(R_{AE})\subseteq\operatorname{supp}(\mathbb{I}_A\otimes L_E) \iff \operatorname{supp}(R_E)\subseteq\operatorname{supp}(L_E)\,.$$

Furthermore, $\operatorname{supp}(\mathbb{I}_A\otimes L_E)=\mathcal{H}_A\otimes\operatorname{supp}(L_E)$.

Proof. We first show "$\Rightarrow$". Consider $|\varphi\rangle\in\ker(L_E)$ and fix an arbitrary vector $|\psi\rangle\in\mathcal{H}_A$. Then, $(\mathbb{I}_A\otimes L_E)|\psi\rangle|\varphi\rangle = |\psi\rangle\otimes L_E|\varphi\rangle = 0$ and so $|\psi\rangle|\varphi\rangle\in\ker(\mathbb{I}_A\otimes L_E)\subseteq\ker(R_{AE})$, where the inclusion in $\ker(R_{AE})$ is by assumption. By the above lemma, $|\varphi\rangle\in\ker(R_E)$.

For "$\Leftarrow$", exploiting again the above lemma, we conclude that indeed the assumption implies that $\ker(\mathbb{I}_A\otimes L_E)=\mathcal{H}_A\otimes\ker(L_E)\subseteq\mathcal{H}_A\otimes\ker(R_E)\subseteq\ker(R_{AE})$.

The final claims is obtained from $\mathcal{H}_A\otimes\ker(L_E)=\ker(\mathbb{I}_A\otimes L_E)$, taking orthogonal complements and noting that $(\mathcal{H}_A\otimes\ker(L_E))^\perp=\mathcal{H}_A\otimes\ker(L_E)^\perp$. □

Lemma 8.3. *For any* $\rho_{AE}\in\mathcal{D}(AE)$ *and* $\sigma_E\in\mathcal{D}(E)$ *with* $\operatorname{supp}(\rho_E)\subseteq\operatorname{supp}(\sigma_E)$

$$\mathrm{H}_\infty(\rho_{AE}|\sigma_E) = -\log\lambda_{\max}\big(\sigma_E^{-1/2}\rho_{AE}\sigma_E^{-1/2}\big) = -\log\big\|\sigma_E^{-1/2}\rho_{AE}\sigma_E^{-1/2}\big\|_\infty\,,$$

where the negative square root of σ_E *is by means of its pseudo-inverse.*

Proof. Since by assumption and Corollary 8.2, $\operatorname{supp}(\rho_{AE})\subseteq\operatorname{supp}(\mathbb{I}_A\otimes\sigma_E)=\mathcal{H}_A\otimes\operatorname{supp}(\sigma_E)$, the definition of $\mathrm{H}_\infty(\rho_{AE}|\sigma_E)$ as well as the claimed value are not affected when replacing $\mathcal{H}_E$ by $\operatorname{supp}(\sigma_E)$ and considering the corresponding restrictions of ρ_{AE} and σ_E. Therefore, we may assume without loss of generality that σ_E has full rank, and thus is invertible. Then, we see that

$$\lambda\cdot\mathbb{I}_A\otimes\sigma_E\ge\rho_{AE} \iff \lambda\cdot\mathbb{I}_A\otimes\mathbb{I}_E\ge\sigma_E^{-1/2}\rho_{AE}\sigma_E^{-1/2} \iff \lambda\ge\big\|\sigma_E^{-1/2}\rho_{AE}\sigma_E^{-1/2}\big\|_\infty\,,$$

where the second equivalence is easily seem by bringing $\sigma_E^{-1/2}\rho_{AE}\sigma_E^{-1/2}$ into diagonal form. □

Remark 8.2. If $\lambda\cdot\mathbb{I}_A\otimes\sigma_E\ge\rho_{AE}$ for a $\sigma_E\in\mathcal{D}(E)$ with $\operatorname{supp}(\rho_E)\subsetneq\operatorname{supp}(\sigma_E)$ then we can consider

$$\tilde\sigma_E := \frac{\rho_E^0\sigma_E\rho_E^0}{\operatorname{tr}(\rho_E^0\sigma_E\rho_E^0)}\in\mathcal{D}(E)\,,$$

which satisfies $\mathrm{supp}(\tilde\sigma_E) = \mathrm{supp}(\rho_E)$. Furthermore, using Remark 0.2,

$$\lambda \cdot \mathrm{tr}(\rho_E^0 \sigma_E \rho_E^0) \cdot \mathbb{I}_A \otimes \tilde\sigma_E \geq \lambda \cdot \mathbb{I}_A \otimes \rho_E^0 \sigma_E \rho_E^0 \geq \rho_E^0 \rho_{AE} \rho_E^0 = \rho_{AE} \, .$$

Given that $\mathrm{tr}(\rho_E^0 \sigma_E \rho_E^0) \leq \|\rho_E^0\|_\infty \|\sigma_E\|_1 = 1$ we thus have that $\mathrm{H}_\infty(\rho_{AE}|\tilde\sigma_E) \geq \mathrm{H}_\infty(\rho_{AE}|\sigma_E)$.

Definition 8.3. *For any $\rho_{AE} \in \mathcal{D}(AE)$, the* **conditional min-entropy** *of A* **given** *E is defined as*

$$\mathrm{H}_\infty(A|E) := \sup_{\sigma_E} \mathrm{H}_\infty(\rho_{AE}|\sigma_E) = \max_{\sigma_E} \mathrm{H}_\infty(\rho_{AE}|\sigma_E)$$

where the supremum/maximum is over all $\sigma_E \in \mathcal{D}(E)$.

Remark 8.3. By Remarks 8.1 and 8.2, the quantification can be restricted to $\sigma_E \in \mathcal{D}(E)$ with $\mathrm{supp}(\sigma_E) = \mathrm{supp}(\rho_E)$, and thus with $\mathrm{supp}(\sigma_E) \subseteq \mathrm{supp}(\rho_E)$. In other words, we may assume without loss of generality that $\mathcal{H}_E = \mathrm{supp}(\rho_E)$. Furthermore, given that the supremum is over a compact set and the objective function is continuous on that set (including the points where the function is $-\infty$), the supremum is attained; thus, writing max is justified.

In case $E = \emptyset$, i.e., $\mathcal{H}_E = \mathbb{C}$, we obviously have $\mathrm{H}_\infty(A|E) = \lambda_{\max}(\rho_A) = \mathrm{H}_\infty(A)$. Also, in case of a product state $\rho_{AE} = \rho_A \otimes \rho_E$, we see that $\mathrm{H}_\infty(\rho_{AE}|\rho_E) = \lambda_{\max}(\rho_A) = \mathrm{H}_\infty(A)$; furthermore, strong subadditivity below implies that $\mathrm{H}_\infty(A|E) \leq \mathrm{H}_\infty(A)$, and thus we have $\mathrm{H}_\infty(A|E) = \mathrm{H}_\infty(A)$. For an arbitrary $\rho_{AE} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_E)$, we note that strong subadditivity implies that $\mathrm{H}_\infty(A|E)$ is still upper bounded by $\log\dim(\mathcal{H}_A)$, and the bound is attained for states of the form $\rho_{AE} = \mu_A \otimes \rho_E = \frac{1}{\dim(\mathcal{H}_A)}\mathbb{I}_A \otimes \rho_E$. On the other hand, looking at the lower bound, it turns out that $\mathrm{H}_\infty(A|E)$ may be *negative*!—though not smaller than $-\log\dim(\mathcal{H}_A)$. This is again an artifact of entanglement. For instance, an EPR pair AE has $\mathrm{H}_\infty(A|E) = -1$, as we will see later.

Considering the case of a *classical* system conditioned on a quantum system, it is easy to see that if $\rho_{XE} \in \mathcal{D}(\mathcal{X} \otimes \mathcal{H}_E)$ is a hybrid state with classical X then

$$\mathbb{I}_X \otimes \rho_E = \sum_x |x\rangle\langle x| \otimes \rho_E \geq \sum_x |x\rangle\langle x| \otimes P_X(x)\rho_{E|X=x} = \rho_{XE} \, ,$$

and thus $\mathrm{H}_\infty(X|E) \geq 0$, so this strange behavior does not occur here—because there is no entanglement. Intuitively, if A and E *are* entangled then ρ_{AE} is not a block-diagonal matrix (and cannot be written as one), like in case of a hybrid state ρ_{XE} above, but it still needs to be "covered" by a block-diagonal matrix, namely by a multiple of $\mathbb{I}_A \otimes \sigma_E$, and thus the latter needs to be "raised higher up". Note that in the case of a hybrid state ρ_{XE}, we can also write

$$\mathrm{H}_\infty(\rho_{XE}|\sigma_E) = -\log \max_x P_X(x) \, \lambda_{\max}\big(\sigma_E^{-1/2} \rho_{E|X=x} \, \sigma_E^{-1/2}\big)$$

The following shows that **monotonicity** is recovered for *classical* subsystems.

Proposition 8.4. *Let $\rho_{XAE} \in \mathcal{D}(\mathcal{X} \otimes \mathcal{H}_A \otimes \mathcal{H}_E)$ and $\sigma_E \in \mathcal{D}(\mathcal{H}_E)$. Then*

$$\mathrm{H}_\infty(\rho_{XAE}|\sigma_E) \geq \mathrm{H}_\infty(\rho_{AE}|\sigma_E) \, .$$

Proof. Let $\lambda > 0$ be minimal such that $\lambda \cdot \mathbb{I}_A \otimes \sigma_E \geq \rho_{AE}$, and thus $\mathrm{H}_\infty(\rho_{AE}|\sigma_E) = -\log\lambda$. Note that $\rho_{AE} = \sum_x P_X(x)\rho_{AE|X=x}$, and thus $\rho_{AE} \geq P_X(x)\rho_{AE|X=x}$ for all x. It then follows that

$$\lambda \cdot |x\rangle\langle x| \otimes \mathbb{I}_A \otimes \sigma_E \geq P_X(x)|x\rangle\langle x| \otimes \rho_{AE|X=x} \, .$$

Summing over all x yields that $\lambda \cdot \mathbb{I}_X \otimes \mathbb{I}_A \otimes \sigma_E \geq \rho_{XAE}$, which proves the claim. □

The following **data-processing inequality** is another natural property: acting on the given system can only make the entropy larger. This in particular implies **strong subadditivity** (as in point 2. of Lemma A.4): $\mathrm{H}_\infty(A|BE) \leq \mathrm{H}_\infty(A|E)$ for every $\rho_{ABE} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$.

Proposition 8.5. *Let $\rho_{AE} \in \mathcal{D}(AE)$, $\sigma_E \in \mathcal{D}(E)$ and $\mathfrak{T} \in \mathcal{L}\big(\mathcal{L}(E), \mathcal{L}(E')\big)$ a CPTP map. Then*

$$\mathrm{H}_\infty\big(\mathfrak{T}_E(\rho_{AE})\big|\mathfrak{T}_E(\sigma_E)\big) \geq \mathrm{H}_\infty(\rho_{AE}|\sigma_E)\,.$$

Proof. Let $\lambda > 0$ be minimal such that $\lambda \cdot \mathbb{I}_A \otimes \sigma_E - \rho_{AE} \geq 0$, and thus $\mathrm{H}_\infty(\rho_{AE}|\sigma_E) = -\log\lambda$. Because $\mathfrak{T}$ is a CPTP map, also $\lambda \cdot \mathbb{I}_A \otimes \mathfrak{T}_E(\sigma_E) - \mathfrak{T}_E(\rho_{AE}) \geq 0$, which proves the claim. □

Motivated by the classical definition, let us also here write $\mathrm{Guess}(A|E)$ for $2^{-\mathrm{H}_\infty(A|E)}$, keeping in mind though that $\mathrm{Guess}(A|E)$ may not be a probability: it may be greater than 1.

Lemma 8.6. *For any hybrid state $\rho_{YAE} \in \mathcal{D}(\mathcal{Y} \otimes \mathcal{H}_A \otimes \mathcal{H}_E)$ with classical Y we have*

$$\mathrm{Guess}(A|YE) = \sum_y P_Y(y)\,\mathrm{Guess}(A|E, Y\!=\!y)\,,$$

with $\mathrm{Guess}(A|E, Y\!=\!y)$ *defined by means of the state* $\rho_{AE|Y=y}$.

In particular, choosing $E = \emptyset$ and a classical A (referred to as X then), we see that in case of a fully classical state ρ_{XY}, the quantum conditional min-entropy coincides with its classical counterpart. As a matter of fact, for a classical X but a (possibly) quantum E, $\mathrm{Guess}(X|E)$ does coincide with the (optimized) guessing probability of guessing X when given E, i.e.

$$\mathrm{Guess}(X|E) = \sup_{\{M_x\}} \sum_x P_X(x)\,\mathrm{tr}(M_x^\dagger M_x \rho_E^x)$$

where the supremum is over all measurements $\{M_x\}_{x\in\mathcal{X}}$. The proof is by means of the strong duality property of so-called semidefinite programs; we do not treat this here.

Proof (of Lemma 8.6). By Proposition 8.5, in $\mathrm{Guess}(A|YE) = \min_{\sigma_{YE}} \lambda_{\max}(\sigma_{YE}^{-1/2}\,\rho_{YAE}\,\sigma_{YE}^{-1/2})$ it is good enough minimize over all σ_{YE} with classical Y; indeed, if Y is not classical then we may measure Y, i.e., apply the CPTP map that captures a measurement in the considered basis, which does not affect the state of ρ_{YAE} as there Y is already classical. Thus,

$$\begin{aligned}
\mathrm{Guess}(A|YE) &= \min_{Q_Y} \min_{\{\sigma_{E|Y=y}\}} \max_y \frac{P_Y(y)}{Q_Y(y)}\,\lambda_{\max}\big(\sigma_{E|Y=y}^{-1/2}\,\rho_{AE|Y=y}\,\sigma_{E|Y=y}^{-1/2}\big)\\
&= \min_{Q_Y} \max_y \frac{P_Y(y)}{Q_Y(y)} \min_{\sigma_{E|Y=y}} \lambda_{\max}\big(\sigma_{E|Y=y}^{-1/2}\,\rho_{AE|Y=y}\,\sigma_{E|Y=y}^{-1/2}\big)\\
&= \min_{Q_Y} \max_y \frac{P_Y(y)}{Q_Y(y)}\,\mathrm{Guess}(A|E, Y\!=\!y)\,.
\end{aligned}$$

We now solve this optimization problem. For this, we observe that the choice of Q_Y for which $\max_y$ is smallest is such that the values $\max_y$ is over are all equal. As such, the minimum is achieved for

$$Q_Y(y) = \frac{P_Y(y)\,\mathrm{Guess}(A|E, Y\!=\!y)}{\sum_{y'} P_Y(y')\,\mathrm{Guess}(A|E, Y\!=\!y')}$$

and it results in the claimed expression. □

Together with strong subadditivity, this implies the following.