Chapter 9

Applications

9.1 Entropic Uncertainty Relations

The famous Heisenberg uncertainty principle states that it is not possible to have a subatomic particle, such as an electron, with a definite position *and* momentum: at least one of the two must have some inherent uncertainty. Using the language of these notes, this translates into the following: for any pair of "sufficiently incompatible" measurements $\mathbf{M}$ and $\mathbf{N}$ and for any state $|\varphi\rangle$, at least one of the two induced probability distributions, given by $p_i = \langle\varphi|M_i^\dagger M_i|\varphi\rangle$ and $q_i = \langle\varphi|N_i^\dagger N_i|\varphi\rangle$, must have substantial entropy. For example, if $|\varphi\rangle \in \mathcal{S}(\mathbb{C}^2)$ is an arbitrarily qubit and X is the random variable discribing the measurement outcome when measuring $|\varphi\rangle$ in the computational basis, i.e., $\mathbf{M} = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, and Y is the random variable discribing the measurement outcome when measuring $|\varphi\rangle$ in the Hadamard basis, i.e., $\mathbf{N} = \{|+\rangle\langle +|, |-\rangle\langle -|\}$, then the **entropic uncertainty relation**

$$\mathrm{H}(X) + \mathrm{H}(Y) \geq 1$$

holds, where H is the Shannon entropy (Definition A.2). This generalizes to an arbitrary state space $\mathcal{H}$ and arbitrary (full-rank) projective measurements, where the inequality then becomes

$$\mathrm{H}(X) + \mathrm{H}(Y) \geq -\log c$$

with c given by the following measure of "incompatability" of two full-rank projective measurements, given by orthonormal bases.[1] The above inequality is knows as the **Maassen-Uffink** entropic uncertainty relation.

Definition 9.1. *The* **overlap** *of two orthonormal bases* $\{|e_x\rangle\}_{x\in\mathcal{X}}$ *and* $\{|f_y\rangle\}_{y\in\mathcal{Y}}$ *is defined as*

$$c := \max_{x,y} |\langle e_x|f_y\rangle|^2 \,,$$

i.e., the square of the maximal fidelity.

The goal of this section is to prove a generalization of the Maassen-Uffink entropic uncertainty relation. Our version generalizes the original relation in two direction: it considers additional "quantum side information" and it is expressed in terms of the general Rényi entropy.

Let $\{|e_x\rangle\}_{x\in\mathcal{X}}$ and $\{|f_y\rangle\}_{y\in\mathcal{Y}}$ be two orthonormal bases of $\mathcal{H}_A$, and let $\mathfrak{M}$ and $\mathfrak{N}$ be the CPTP maps describing the corresponding measurements, i.e.,

$$\mathfrak{M}(\rho) = \sum_x |x\rangle\langle e_x|\rho|e_x\rangle\langle x|$$

and correspondingly for $\mathfrak{N}$. We let c be the overlap of $\{|e_x\rangle\}_{x\in\mathcal{X}}$ and $\{|f_y\rangle\}_{y\in\mathcal{Y}}$.

[1]Sometimes, c is defined without the square, in which case that bound becomes $-2\log c$.

Theorem 9.1. *Let $\frac{1}{2} \le \alpha, \beta \le \infty$ with $\frac{1}{\alpha} + \frac{1}{\beta} = 2$, and let $\rho_{ABE} \in \mathcal{D}(ABE)$. Then*

$$\mathrm{H}_\alpha(\mathfrak{M}(A)|B) + \mathrm{H}_\beta(\mathfrak{N}(A)|E) \ge -\log c\,,$$

where $\mathrm{H}_\alpha(\mathfrak{M}(A)|B)$ is understood as $\mathrm{H}_\alpha(X|B)$ for $\rho_{XB} := \mathfrak{M}_{A\to X}(\rho_{AB})$, and similarly $\mathrm{H}_\beta(\mathfrak{N}(A)|E)$.

By considering empty subsystems B and E, and taking $\alpha = \beta = 1$, we obviously recover the original Maassen-Uffink entropic uncertainty relation.

For the proof, we need yet another variant of the data-processing inequality.

Lemma 9.2. *Let $\frac{1}{2} \le \alpha \le \infty$. Then, for any isometry $V \in \mathcal{L}(\mathcal{H}, \mathcal{H} \otimes \mathcal{H}')$ and for $\rho \in \mathcal{D}(\mathcal{H})$ and $\sigma' \in \mathcal{P}(\mathcal{H} \otimes \mathcal{H}')$:*

$$\mathrm{D}_\alpha(V\rho V^\dagger \| \sigma') \ge \mathrm{D}_\alpha(\rho \,\| V^\dagger \sigma' V)\,.$$

Proof. Let $|0\rangle$ be an arbitrary fixed state in $\mathcal{S}(\mathcal{H}')$. Given that $\mathbb{I} \otimes |0\rangle$ is an isometry as well, V can be written as $V = U(\mathbb{I} \otimes |0\rangle)$ for a unitary $U \in \mathcal{U}(\mathcal{H} \otimes \mathcal{H}')$. Therefore, $V^\dagger = (\mathbb{I} \otimes \langle 0|)U^\dagger$ and thus $V^\dagger \otimes |0\rangle = (\mathbb{I} \otimes |0\rangle)V^\dagger = (\mathbb{I} \otimes |0\rangle\langle 0|)U^\dagger$. In words: $V^\dagger$ followed by "attaching" $|0\rangle$ equals a unitary followed by a projection. Observing that

$$V\rho V^\dagger = U(\rho \otimes |0\rangle)(\mathbb{I} \otimes \langle 0|)U^\dagger = U(\rho \otimes |0\rangle\langle 0|)U^\dagger$$

we thus use Lemma 8.20, and basic properties of D_α, to argue that

$$\begin{aligned}
\mathrm{D}_\alpha(V\rho V^\dagger \| \sigma') &= \mathrm{D}_\alpha\big(U(\rho \otimes |0\rangle\langle 0|)U^\dagger \| \sigma'\big) \\
&= \mathrm{D}_\alpha\big(\rho \otimes |0\rangle\langle 0| \| U^\dagger \sigma' U\big) \\
&\ge \mathrm{D}_\alpha\big(\rho \otimes |0\rangle\langle 0| \| (\mathbb{I} \otimes |0\rangle\langle 0|)U^\dagger \sigma' U(\mathbb{I} \otimes |0\rangle\langle 0|)\big) \\
&= \mathrm{D}_\alpha\big(\rho \otimes |0\rangle\langle 0| \| V^\dagger \sigma' V \otimes |0\rangle\langle 0|\big) \\
&= \mathrm{D}_\alpha\big(\rho \| V^\dagger \sigma' V\big)\,,
\end{aligned}$$

which was to be proven. □

Proof of Theorem 9.1. We may assume $\alpha > 1$. The case $\alpha < 1$ follows by symmetry, and the case $\alpha = 1$ by taking the limit. Consider the isometry

$$V = \sum_y |y\rangle\langle f_y| \otimes |y\rangle \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_Y \otimes \mathcal{H}_{Y'})$$

where $\mathcal{H}_Y = \mathcal{H}_{Y'} = \mathcal{H}_A$. It is easy to verify that, as a CPTP map, V satisfies $\mathrm{tr}_{Y'} \circ V = \mathfrak{N}$; in particular, setting $\rho_{YY'BE} = V_{A\to YY'}(\rho_{ABE})$ we have $\rho_{YBE} = \mathfrak{N}_{A\to Y}(\rho_{ABE}) = \mathrm{tr}_{Y'}(\rho_{YY'BE})$. In other words, V is the isometry $U(\mathbb{I} \otimes |0\rangle)$ from the Stinespring representation of $\mathfrak{N}$. It then follows from the duality relation (Theorem 8.17) that $\mathrm{H}_\beta(\mathfrak{N}(A)|E) = \mathrm{H}_\beta(Y|E) \ge -\mathrm{H}_\alpha(Y|Y'B)$.

For a suitable $\sigma_{Y'B}$, taking it as understood that V acts on A and $V^\dagger$ on YY', we have

$$-\mathrm{H}_\alpha(Y|Y'B) = \mathrm{D}_\alpha(\rho_{YY'B} \,\|\, \mathbb{I}_Y \otimes \sigma_{Y'B}) = \mathrm{D}_\alpha\big(V(\rho_{AB}) \| \, \mathbb{I}_Y \otimes \sigma_{Y'B}\big)\,,$$

and thus by Lemma 9.2 and by the (ordinary) data-processing inequality (Theorem 8.13),

$$-\mathrm{H}_\alpha(Y|Y'B) \ge \mathrm{D}_\alpha\big(\rho_{AB} \,\| V^\dagger(\mathbb{I}_Y \otimes \sigma_{Y'B})\big) \ge \mathrm{D}_\alpha\big(\rho_{XB} \,\| \mathfrak{M} \circ V^\dagger(\mathbb{I}_Y \otimes \sigma_{Y'B})\big)$$

Working out the right-hand-side argument of D_α, we obtain

$$\mathfrak{M} \circ V^\dagger(\mathbb{I}_Y \otimes \sigma_{Y'B}) = \sum_{x,y} |x\rangle\langle e_x|f_y\rangle\langle f_y|e_x\rangle\langle x| \otimes \langle y|\sigma_{Y'B}|y\rangle \le c \cdot \mathbb{I}_X \otimes \sigma_B\,,$$

with $\sigma_B = \mathrm{tr}_{Y'}(\sigma_{Y'B})$. Hence, by the operator anti-monotonicity of $x \mapsto x^{\frac{1-\alpha}{\alpha}}$ (Theorem B.2) and by the monotonicity of the Schatten norm (Corollary 7.3),

$$\mathrm{D}_\alpha\big(\rho_{XB}\,\|\,\mathfrak{M}\circ V^\dagger(\mathbb{I}_Y\otimes\sigma_{Y'B})\big) \geq \mathrm{D}_\alpha(\rho_{XB}\,\|\,c\cdot\mathbb{I}_X\otimes\sigma_B)$$

and therefore

$$-\mathrm{H}_\alpha(Y|Y'B) \geq \mathrm{D}_\alpha(\rho_{XB}\,\|\,c\cdot\mathbb{I}_X\otimes\sigma_B) \geq \mathrm{D}_\alpha(\rho_{XB}\,\|\,\mathbb{I}_X\otimes\sigma_B) - \log c \geq -\mathrm{H}_\alpha(X|B) - \log c\,.$$

Recalling that $\mathrm{H}_\beta(Y|E) \geq -\mathrm{H}_\alpha(Y|Y'B)$ then concludes the proof. □

9.2 Privacy Amplification

We conclude with **privacy amplification**, also known as **randomness extraction**. The objective is to transform a *weak* (classical) source of randomness X, that may be correlated to (quantum) side information E, into an *almost perfect* and *uncorrelated* source of randomness. We show here that this is possible as soon as there is *some* uncertainty in X given E, formally captured by having a lower bound on $\mathrm{H}_2(X|E)$. The transformation itself requires some randomness as a "catalyst" but is fully public, no secrecy is involved.

The considered privacy amplification procedure is by means of *universal hashing*, which we quickly introduce here. Let $\mathcal{S},\mathcal{X}$ and $\mathcal{K}$ be arbitrary non-empty, finite sets.

Definition 9.2. *A function $f:\mathcal{S}\times\mathcal{X}\to\mathcal{K}$ is called* **universal** *if for every pair $x\neq x'\in\mathcal{X}$*

$$\big|\{s\in\mathcal{S}\,|\,f(s,x)=f(s,x')\}\big| \leq \frac{|\mathcal{S}|}{|\mathcal{K}|}\,.$$

The first argument is typically called the **seed**, and the second is sometimes referred to as **actual input**. The seed should be chosen uniformly at random, independent of X and E, but may be "publicly known".

IN the language of probability theory, $f:\mathcal{S}\times\mathcal{X}\to\mathcal{K}$ is universal if and only if

$$P\big[f(S,x)=f(S,x')\big] \leq \frac{1}{|\mathcal{K}|} \quad \forall\, x\neq x'\in\mathcal{X}$$

when S be uniformly distributed over $\mathcal{S}$. In other words, the probability that two distinct actual inputs *collide* under a random seed is no bigger than for two random elements in the range $\mathcal{K}$.

Although a universal function does not have to be *hashing* (in the sense of $|\mathcal{K}|<|\mathcal{X}|$), they are usually referred to as universal *hash* functions. Examples of universal (hash) functions are

$$f:\mathbb{F}^{\ell\times n}\times\mathbb{F}^n\to\mathbb{F}^\ell,\ (A,x)\mapsto Ax$$

with $\ell\leq n$ and where $\mathbb{F}$ is an arbitrary finite field, and

$$f:\mathbb{F}_{p^n}\times\mathbb{F}_{p^n}\to\mathbb{F}_p^\ell,\ (a,x)\mapsto[a\cdot x]_\ell\,,$$

with $\ell\leq n$ and where $\mathbb{F}_q$ stands for the finite field with q elements, and $[\,\cdot\,]_\ell:\mathbb{F}_{p^n}\to\mathbb{F}_p^\ell$ is an arbitrary surjective $\mathbb{F}_p$-linear map (e.g. $[\,\cdot\,]_\ell=$ the first ℓ coordinates w.r.t. a $\mathbb{F}_p$-basis of $\mathbb{F}_{p^n}$).

Theorem 9.3 (Privacy amplification)**.** *Let $\rho_{XE}\in\mathcal{D}(\mathcal{X}\otimes\mathcal{H}_E)$. Let $f:\mathcal{S}\times\mathcal{X}\to\mathcal{K}=\{0,1\}^\ell$ be a universal hash function and $\mu_S=\frac{1}{|\mathcal{S}|}\mathbb{I}_S$ the density operator representation of the uniform distribution over $\mathcal{S}$. Consider $\rho_{SXE}=\mu_S\otimes\rho_{XE}\in\mathcal{D}(\mathcal{S}\otimes\mathcal{X}\otimes\mathcal{H}_E)$. Then*

$$\delta\big(\rho_{f(S,X)SE},\mu_K\otimes\rho_{SE}\big) \leq \frac{1}{2}\,2^{-\frac{1}{2}(\mathrm{H}_2(X|E)-\ell)} \leq \frac{1}{2}\,2^{-\frac{1}{2}(\mathrm{H}_\infty(X|E)-\ell)}\,,$$

where $\mu_K=\frac{1}{2^\ell}\mathbb{I}_K$ is the density operator representation of the uniform distribution over $\mathcal{K}$.

Informally, this means that up to some gap that determines the "error" — and the error decreases exponentially fast in this gap — $\mathrm{H}_2(X|E)$ almost-random bits can be extracted. For the proof, we need the following technical observation.

Lemma 9.4. *For any Hermitian $R \in \mathcal{L}(\mathcal{H})$ and any $L \in \mathcal{L}(\mathcal{H})$: $\mathrm{tr}|LRL^\dagger| \leq \mathrm{tr}(L|R|L^\dagger)$.*

Proof. Consider the spectral decompositions $R = \sum_i \lambda_i |e_i\rangle\langle e_i|$ and $LRL^\dagger = \sum_j \mu_j |f_j\rangle\langle f_j|$. Then

$$\begin{aligned}\mathrm{tr}|LRL^\dagger| &= \sum_j |\mu_j| = \sum_j \big|\langle f_j|LRL^\dagger|f_j\rangle\big| = \sum_j \Big|\sum_i \lambda_i \langle f_j|L|e_i\rangle\langle e_i|L^\dagger|f_j\rangle\Big| \\ &\leq \sum_j \sum_i |\lambda_i| \langle f_j|L|e_i\rangle\langle e_i|L^\dagger|f_j\rangle = \sum_j \langle f_j|L|R|L^\dagger|f_j\rangle = \mathrm{tr}(L|R|L^\dagger)\,,\end{aligned}$$

which was to be proven. □

Proof of Theorem 9.3. We write K for $f(S,X)$ so that $\rho_{KSE} = \rho_{f(S,X)SE}$. First, we note that by Lemma 7.8 and using the fact that S is independent of X and E,

$$\delta := \delta\big(\rho_{KSE}, \mu_K \otimes \rho_{SE}\big) = \sum_s P_S(s)\delta\big(\rho^s_{f(S,X)E}, \mu_K \otimes \rho^s_E\big) = \sum_s P_S(s)\delta\big(\rho_{f(s,X)E}, \mu_K \otimes \rho_E\big)\,.$$

Furthermore, using Lemma 9.4 and Hölder inequality (Theorem 7.1), for any density operator $\sigma_E \in \mathcal{D}(\mathcal{H}_E)$ with $\mathrm{supp}(\rho_E) \subseteq \mathrm{supp}(\sigma_E)$ we have

$$\begin{aligned}\delta\big(\rho_{f(s,X)E}, \mu_K \otimes \rho_E\big) &= \frac{1}{2}\,\mathrm{tr}\big|\sigma_E^{1/4}\sigma_E^{-1/4}(\rho_{f(s,X)E} - \mu_K \otimes \rho_E)\sigma_E^{-1/4}\sigma_E^{1/4}\big| \\ &\leq \frac{1}{2}\,\mathrm{tr}\big(\sigma_E^{1/4}\big|\sigma_E^{-1/4}(\rho_{f(s,X)E} - \mu_K \otimes \rho_E)\sigma_E^{-1/4}\big|\sigma_E^{1/4}\big) \\ &\leq \frac{1}{2}\,\big\|\mathbb{I}_K \otimes \sigma_E^{1/2}\big\|_2 \cdot \big\|\sigma_E^{1/4}(\rho_{f(s,X)E} - \mu_K \otimes \rho_E)\sigma_E^{1/4}\big\|_2 \\ &= \frac{1}{2}\sqrt{2^\ell\,\mathrm{tr}\big((\rho_{f(s,X)E} - \mu_K \otimes \rho_E)\sigma_E^{-1/2}(\rho_{f(s,X)E} - \mu_K \otimes \rho_E)\sigma_E^{-1/2}\big)}\end{aligned}$$

Applying Jensen inequality (Proposition B.5), we thus obtain

$$\delta \leq \frac{1}{2}\sqrt{\sum_s P_S(s)\,2^\ell\,\mathrm{tr}\big((\rho_{f(s,X)E} - \mu_K \otimes \rho_E)\sigma_E^{-1/2}(\rho_{f(s,X)E} - \mu_K \otimes \rho_E)\sigma_E^{-1/2}\big)}\,.$$

Multiplying out the product in the trace, noting that $\sum_s P_S(s)\rho_{f(s,X)E} = \rho_{KE}$ and $2^\ell \mu_K = \mathbb{I}_K$, and applying Proposition 6.1 to obtain, e.g.,

$$\mathrm{tr}\big(\rho_{KE}\,\sigma_E^{-1/2}\,(2^\ell\mu_K \otimes \rho_E)\,\sigma_E^{-1/2}\big) = \mathrm{tr}\big(\rho_{KE}\,\sigma_E^{-1/2}\rho_E\,\sigma_E^{-1/2}\big) = \mathrm{tr}\big((\rho_E\,\sigma_E^{-1/2})^2\big)\,,$$

we then get

$$4\delta^2 \leq 2^\ell \sum_s P_S(s)\,\mathrm{tr}\big((\rho_{f(s,X)E}\,\sigma_E^{-1/2})^2\big) - \mathrm{tr}\big((\rho_E\,\sigma_E^{-1/2})^2\big)\,.$$

Writing $\rho_{f(s,X)E} = \sum_x P_X(x)|f(s,x)\rangle\langle f(s,x)| \otimes \rho^x_E$, we see that

$$\mathrm{tr}\big((\rho_{f(s,X)E}\,\sigma_E^{-1/2})^2\big) = \sum_{x,x'} P_X(x)P_X(x')\,\big\langle f(s,x)\big|f(s,x')\big\rangle\,\mathrm{tr}\big(\rho^x_E\,\sigma_E^{-1/2}\rho^{x'}_E\,\sigma_E^{-1/2}\big)$$

and therefore, by splitting up the sum into one with $x \neq x'$ and one with $x = x'$, and observing that $\sum_s P_S(s)\langle f(s,x)|f(s,x')\rangle = P[f(S,x) = f(S,x')] \leq 2^{-\ell}$, we get

$$2^\ell \sum_s P_S(s)\,\mathrm{tr}\big(\rho^x_E\,\sigma_E^{-1/2}\rho^{x'}_E\,\sigma_E^{-1/2}\big)$$

$$\leq \sum_{x \neq x'} P_X(x) P_X(x') \,\mathrm{tr}\big(\rho_E^x \,\sigma_E^{-1/2} \rho_E^{x'} \,\sigma_E^{-1/2}\big) + 2^\ell \sum_x P_X(x)^2 \,\mathrm{tr}\big((\rho_E^x \sigma_E^{-1/2})^2\big)$$
$$= \mathrm{tr}\big((\rho_E \sigma_E^{-1/2})^2\big) + (2^\ell - 1)\mathrm{tr}\big((\rho_{XE} \sigma_E^{-1/2})^2\big) \,,$$

where for the inequality we use that $\mathrm{tr}\big(\rho_E^x \,\sigma_E^{-1/2} \rho_E^{x'} \sigma_E^{-1/2}\big) = \mathrm{tr}\big(\sigma_E^{-1/4} \rho_E^x \,\sigma_E^{-1/4} \,\sigma_E^{-1/4} \rho_E^{x'} \sigma_E^{-1/4}\big) \geq 0$. Therefore,

$$\delta\big(\rho_{f(S,X)SE}, \mu_K \otimes \rho_{SE}\big)^2 \leq \frac{1}{2}\sqrt{2^\ell \,\mathrm{tr}\big(\sigma_E^{-1/2} \rho_{XE} \,\sigma_E^{-1/2} \rho_{XE}\big)} = \frac{1}{2} 2^{-\frac{1}{2}(\mathrm{H}_2(\rho_{XE}|\sigma_E) - \ell)} \,.$$

The claim thus follows by definition of $\mathrm{H}_2(X|E)$, and as it upper bounds $\mathrm{H}_\infty(X|E)$. □