Self-Study Notes on Smooth Entropies and One-Shot Quantum Information

Sareh Askari

A small note for readers. These notes are my personal attempt to understand smooth entropies and their role in one-shot quantum information theory. I originally worked through these ideas over several months in scattered notebooks and loose files. I recently took some time to organize everything cleanly and share it here in case anyone else finds it useful or enjoyable. If you have suggestions or want to discuss ideas, feel free to reach out: `Sareh.askari17@gmail.com`.

Outline

1. Why ordinary entropy is not enough in one-shot scenarios
2. Classical min- and max-entropy: intuition and definitions
3. Smooth entropies $H_{\min}^{\varepsilon}$ and $H_{\max}^{\varepsilon}$
4. The operational meaning of $H_{\min}$: guessing probability
5. Toy examples to build intuition
6. A short note on the quantum case

—

1 Why smooth entropies?

In the usual information-theoretic setting, we work in the *asymptotic* regime: long sequences of independent copies, many uses of a channel, and coding theorems that describe behavior in the limit of large block length. Shannon entropy (classical) and von Neumann entropy (quantum) naturally arise there.

But many practical tasks—especially in cryptography or small-scale quantum devices—are *one-shot*: we only have one or a few samples. In this regime, the standard entropy no longer describes operational quantities reliably.

Renner introduced the **smooth min-entropy** and **smooth max-entropy** to handle precisely these situations. These entropies measure uncertainty in a way that is robust to small errors and directly tied to operational tasks like:

- randomness extraction, - data compression with side information, - security of key distribution, - state merging and decoupling.

The core idea is simple but powerful:

> Smooth entropies describe uncertainty and information-processing power in a single instance, not in the limit of many repetitions.

—

2 Classical min-entropy and max-entropy

Let X be a classical random variable with distribution $p(x)$.

The classical Shannon entropy is

$$H(X) = -\sum_x p(x) \log_2 p(x),$$

which describes average uncertainty when many independent copies of X are considered.

But in one-shot scenarios, two alternative entropies are more meaningful:

Min-entropy

$$H_{\min}(X) = -\log_2 \big(\max_x p(x) \big).$$

This depends only on the *most likely outcome*. If one outcome has high probability, then the min-entropy is small.

Min-entropy is tightly linked to *guessing probability*:

$$P_{\text{guess}}(X) = \max_x p(x) = 2^{-H_{\min}(X)}.$$

Max-entropy

One definition used in the smooth-entropy framework is:

$$H_{\max}(X) = 2 \log_2 \left(\sum_x \sqrt{p(x)} \right).$$

This entropy increases when the distribution spreads out and plays a role in one-shot data compression and uncertainty relations.

—

3 Toy examples

Example 1: Fair coin

$$p = (0.5, 0.5)$$

- $P_{\text{guess}} = 0.5$ - $H_{\min}(X) = 1$ bit - $H_{\max}(X) = 1$ bit (same as Shannon)

Example 2: Biased coin

$$p = (0.9, 0.1)$$

- $P_{\text{guess}} = 0.9$ - $H_{\min}(X) = -\log_2(0.9) \approx 0.152$ bits - Shannon entropy is much larger (≈ 0.47 bits)

This illustrates how min-entropy captures "worst-case" unpredictability rather than average.

—

4 Smooth entropies

The *smooth min-entropy* of X is defined as

$$H_{\min}^{\varepsilon}(X) = \max_{\tilde{p}:\, D(\tilde{p},p)\leq\varepsilon} H_{\min}(\tilde{p}),$$

where the maximization is over distributions $\tilde{p}$ that are ε-close to the original one in purified or trace distance.

Intuition:

- We allow ourselves to "ignore" unlikely events with total probability ε. - After trimming those tails, the remaining distribution is renormalized. - The min-entropy of this trimmed distribution is often larger.

This makes the entropy robust to noise, statistical fluctuations, or rare events.

Toy smoothing intuition

For a distribution like

$$p = (0.6, 0.2, 0.15, 0.05),$$

ignoring the last outcome (probability 0.05) increases the min-entropy from $-\log_2 0.6$ to something closer to $-\log_2 0.5 = 1$.

This matches the real definition qualitatively.

—

5 Operational meaning of min-entropy

One of the nicest interpretations is:

$$H_{\min}(X) = -\log_2 P_{\text{guess}}(X).$$

In other words, min-entropy measures how uncertain X is to someone who wants to guess it in one try.

Applications include:

- optimal guessing strategies, - security in quantum key distribution, - extractable randomness, - privacy amplification.

This also connects deeply to quantum conditional min-entropy and the decoupling approach used in one-shot quantum information theory.

—

6 Short note on the quantum case

For a classical-quantum state

$$\rho_{XB} = \sum_x p(x) \, |x\rangle\langle x| \otimes \rho_B^x,$$

one defines the conditional min-entropy as

$$H_{\min}(X|B) = -\log_2 P_{\text{guess}}(X|B),$$

where $P_{\text{guess}}(X|B)$ is the optimal probability of guessing X given access to the quantum side information B.

This quantity plays an essential role in randomness extraction against quantum adversaries, quantum cryptography, state merging, and decoupling theorems.

Smooth versions $H_{\min}^{\varepsilon}(X|B)$ and $H_{\max}^{\varepsilon}(X|B)$ appear throughout one-shot quantum information theory, especially in Renner's work.

—

Final thoughts

If you're reading these notes, I hope they offer a bit of intuition and enjoyment while exploring smooth entropies. These quantities can initially feel abstract, but they reveal a beautiful idea: *information and uncertainty can be described operationally even in the single-shot regime.* That perspective opens up a surprisingly rich view of quantum information tasks.

Feel free to reach out if you'd like to discuss or share comments: `Sareh.askari17@gmail.com`

References

1. R. Renner, *Security of Quantum Key Distribution*, Ph.D. thesis (ETH Zürich, 2005).