

Homework problem set 2

Please hand in your solutions to these exercises in digital form (typed, or scanned from a neatly hand-written version) through Moodle no later than **Friday June 23, 20:00h**.

Problem 1: Min-Entropy Chain rule for cq-states

Let $\rho_{XE} = \sum_x P_X(x) |x\rangle\langle x| \otimes \rho_E^x$ be a cq-state. Prove the following chain rule:

$$H_{\min}(X|E) \geq H_{\min}(X) - \log |E|.$$

Hint: Use the fact that $0 \leq \rho_E^x \leq \mathbb{1}$.

Problem 2: injective functions are collapsing

Show that an injective function is collapsing, i.e. give a proof of Lemma 2 of [our recent paper](#). You can ignore the oracles \mathcal{O} in the statement of Lemma 2 and in Definition 1.

Problem 3: A weak seeded extractor

For any $y \in \{0, 1\}^n$, define $f_y : \{0, 1\}^n \rightarrow \{0, 1\}^n$ by $f_y(x) = x \oplus y$. Here, \oplus represents the bitwise parity (e.g., $11 \oplus 01 = 10$).

- (a) Show that the family $\mathcal{F} = \{f_y\}$ is 1-universal.
- (b) Show that the family $\mathcal{F} = \{f_y\}$ is not 2-universal.
- (c) How could you use \mathcal{F} to build a $(k, 0)$ -weak seeded randomness extractor $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ for any k . Is this extractor useful?
- (d) Alice and Bob are impressed by the parameter $\epsilon = 0$ in the previous exercise. They decide that if \mathcal{F} can be used for a $(k, 0)$ -weak seeded randomness extractor, then certainly it can reasonably be used as a **strong** seeded randomness extractor as well. They define $\text{Ext}(x, y) = f_y(x)$.

Do you think this is a good idea? How does Eve's guessing probability change after extraction?