

## 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 Canvas no later than **Friday June 23, 20:00h**.

### Problem 1: Injective functions are collapsing

Show that an injective function is collapsing, i.e. give a proof of Lemma 4 of [our recent paper](#). You can ignore the oracles  $\mathcal{O}$  in the statement of Lemma 4 and in Definition 3.

### Problem 2: 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  $0 \leq k \leq n$ ? Is this extractor useful?
- (d) Alice and Bob have a  $k$ -source  $X$  for some  $k < n$ . They are impressed by the parameters in the previous subexercise, and decide to use  $\mathcal{F}$  to build a strong seeded randomness extractor as well. They know they should not expect to securely extract more than  $k$  bits of key, so they define  $\text{Ext}(x, y) := (x_1 \oplus y_1, \dots, x_k \oplus y_k)$ , that is, the first  $k$  bits of  $f_y(x)$ . (From the exercise session, they know how to show that this set of functions is still 1-universal). Do you think this is a good idea? Give a lower bound to Eve's probability of guessing the key.

### Problem 3: 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 4: Min-entropy from the matching outcomes bound

Alice and Bob can extract at most  $H_{\min}(X|E)$  bits of randomness to create their key,  $X$  is the outcome of Alice's measurement on her qubit. Now we want to connect the conditional min-entropy to the probability that the matching-outcomes test succeeds. We assume that the adversary Eve prepares  $n$  identical and uncorrelated copies of the tripartite state  $|\psi_{ABE}\rangle$  and sends the qubits  $A$  to Alice and  $B$  to Bob. Recall that if Alice measures her qubit in the standard basis, and the resulting post-measurement state on her qubit and Eve's system  $E$  is a classical-quantum (cq) state

$$\rho_{XE} = \frac{1}{2} |0\rangle\langle 0| \otimes \rho_E^{Z,0} + \frac{1}{2} |1\rangle\langle 1| \otimes \rho_E^{Z,1}, \quad (1)$$

then the optimal guessing probability  $P_{\text{guess}}(X|E)$  such that

$$H_{\min}(X|E) = -\log P_{\text{guess}}(X|E) \quad (2)$$

is given by the Helström measurement, for which

$$P_{\text{guess}}(X|E) = \frac{1}{2} + \frac{1}{4} \|\rho_E^{Z,0} - \rho_E^{Z,1}\|_1. \quad (3)$$

The same reasoning holds for any other choice of Alice's basis, notably the Hadamard basis  $\{|+\rangle, |-\rangle\}$ . In the BB'84 protocol Alice chooses with probability  $1/2$  one of the two bases in which to measure her qubit. If we denote by  $P_{\text{guess}}(X|E, \Theta = 0)$  and  $P_{\text{guess}}(X|E, \Theta = 1)$  the optimal guessing probabilities for Alice measuring in the standard ( $\Theta = 0$ ) and Hadamard ( $\Theta = 1$ ) bases respectively, the desired lower bound is given by

$$H_{\min}(X|E) = -\log \left[ \frac{1}{2} P_{\text{guess}}(X|E, \Theta = 0) + \frac{1}{2} P_{\text{guess}}(X|E, \Theta = 1) \right]. \quad (4)$$

(a) **Problem 1** Suppose Alice and Bob share a pure Bell pair  $|\Phi^+\rangle$ , uncorrelated with Eve's system:  $\rho_{ABE} = |\Phi^+\rangle\langle\Phi^+|_{AB} \otimes \rho_E$ . What is  $H_{\min}(X|E)$ ?

(b) **Problem 2** Now consider the general case, where  $|\psi_{ABE}\rangle$  is an arbitrary state prepared by Eve. Let  $p$  be the probability that this state succeeds in the matching outcomes test, when Alice and Bob both measure in the same basis  $\Theta$  chosen at random. Give coefficients  $a, b, c$  such that

$$p = a\langle\psi_{ABE}|X_A \otimes X_B \otimes \mathbb{1}_E|\psi_{ABE}\rangle + b\langle\psi_{ABE}|Z_A \otimes Z_B \otimes \mathbb{1}_E|\psi_{ABE}\rangle + c, \quad (5)$$

where  $X, Z$  are the Pauli observables  $X = |+\rangle\langle+| - |-\rangle\langle-|$  and  $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$ .

(c) **Problem 3** Let  $p_X$  (resp.  $p_Z$ ) be the probability that the state  $|\psi_{ABE}\rangle$  passes the matching outcomes test in the Hadamard (resp. computational) basis, so that  $p = \frac{1}{2}(p_X + p_Z)$ .

By expanding the qubit  $A$  in the computational basis, the state  $|\psi_{ABE}\rangle$  can be expressed as  $|\psi_{ABE}\rangle = |0\rangle_A \otimes |u_0\rangle_{BE} + |1\rangle_A \otimes |u_1\rangle_{BE}$  ( $|u\rangle_{BE}$  signifies a not normalized vector in  $\mathcal{H}_{BE}$ ), with  $\| |u_0\rangle_{BE} \|^2 + \| |u_1\rangle_{BE} \|^2 = 1$ . Give coefficients  $a', b'$  such that

$$\langle\psi_{ABE}|X_A \otimes X_B \otimes \mathbb{1}_E|\psi_{ABE}\rangle = a' \Re((u_0|X_B \otimes \mathbb{1}_E|u_1)) + b'. \quad (6)$$

(d) **Problem 4** Suppose Alice measures her qubit in the computational basis: the post-measurement state on  $A$  and  $E$  (tracing out  $B$ ) can be written as  $\rho_{AE}^Z = |0\rangle\langle 0|_A \otimes \sigma_E^{Z,0} + |1\rangle\langle 1|_A \otimes \sigma_E^{Z,1}$ . Similarly, if Alice measures in the Hadamard basis we may write the post-measurement state as  $\rho_{AE}^X = |+\rangle\langle+|_A \otimes \sigma_E^{X,+} + |-\rangle\langle-|_A \otimes \sigma_E^{X,-}$ .

Use the previous two questions to determine coefficients  $\alpha, \beta$  such that

$$2p - 1 \leq \alpha F(\sigma_E^{X,+}, \sigma_E^{X,-}) + \beta F(\sigma_E^{Z,0}, \sigma_E^{Z,1}). \quad (7)$$

where  $F$  denotes the fidelity.

[Hint: observe that  $|u_0\rangle_{BE}$  and  $|u_1\rangle_{BE}$  considered in the previous question are purifications of  $\sigma_E^{Z,0}$  and  $\sigma_E^{Z,1}$  respectively, and use Uhlmann's theorem]

(e) **Problem 5** Recall the inequality  $D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2}$ . Using also the definition of  $H_{\min}(X|E)$  (Equations (3), (4)), show that the best lower

bound on  $H_{\min}(X|E)$ , as a function of  $p$ , that you can get is

$$1 - \log \left( 1 + \sqrt{p(1-p) + \frac{3}{4}} \right). \quad (8)$$