COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise Solution # 4

1. **Using the Pretty-Good Measurement**

   (a) The overall success probability is $\frac{1}{3}\langle +|\,\rho_0\,|+\rangle + \frac{1}{3}\langle -|\,\rho_2\,|-\rangle = \frac{1}{3}$.

   (b) Bob's overall success probability is $\frac{1}{3}\langle 0|\,\rho_0\,|0\rangle + \frac{1}{3}\langle 1|\,\rho_2\,|1\rangle = \frac{2}{3}$.

   (c) Let $\rho = \frac{1}{3}(\rho_0 + \rho_1 + \rho_2) = \frac{1}{2}\mathbb{I}$. The elements of the pretty-good measurement are $M_i = \frac{1}{3}\rho^{-1/2}\rho_i\rho^{-1/2}$. Since $\rho = \frac{1}{2}id$, we have that $\rho^{-1/2} = \sqrt{2}id$. The overall success probability is

   $$\frac{1}{3}\sum_i \mathrm{Tr}(M_i\rho_i) = \frac{2}{9}\sum_i \mathrm{Tr}(\rho_i^2) = \frac{2}{9}\left(1 + \frac{1}{2} + 1\right) = \frac{5}{9}\ .$$

   (d) We check that for each i, $\frac{1}{3}\rho_i \leq \sigma = \frac{1}{3}id$. Indeed,

   $$\frac{1}{3}\rho_0 = \frac{1}{3}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \leq \frac{1}{3}id\ , \qquad \frac{1}{3}\rho_1 = \frac{1}{6}id \leq \frac{1}{3}id\ , \qquad \frac{1}{3}\rho_2 = \frac{1}{3}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \leq \frac{1}{3}id\ .$$

   Thus the upper bound on the guessing probability is thus $\mathrm{Tr}\,\sigma = \frac{2}{3}$.

   (e) If the optimal measurement has POVM elements $\{M_i\}$, then we observe that

   $$\begin{aligned}\sum_i p_i \mathrm{Tr}(M_i\sigma_i) &= \sum_i \mathrm{Tr}(M_i \cdot (p_i\sigma_i)) \\ &\leq \sum_i \mathrm{Tr}(M_i\sigma) \\ &= \mathrm{Tr}\Big(\Big(\sum_i M_i\Big)\sigma\Big) \\ &= \mathrm{Tr}(\sigma)\ .\end{aligned}$$

   Here, for the second line we used that if $\rho \leq \sigma$ then for any positive semidefinite M, $\mathrm{Tr}(M(\sigma - \rho)) \geq 0$, i.e. $\mathrm{Tr}(M\rho) \leq \mathrm{Tr}(M\sigma)$.

2. **Deterministic Extractors on Bit-Fixing Sources**

   (a) We can think of generating X_0 by $n - t$ independent fair coin flips, so each of its strings occurs with equal probability 2^{t-n} and $H_{\min}(X_0) = -\log 2^{t-n} = n - t$.

   (b) The number of strings with an even number of 0s is equal to the number of strings with an odd number of 0s, so each of these is equal to 2^{n-1}. Thus the min-entropy of X_1 is $-\log\frac{1}{2^{n-1}} = (n-1)$.

(c) As before, think of generating X_2 through a series of independent fair coin flips: it is fully determined by $\frac{n}{2}$ of them and so $H_{\min}(X_2) = \frac{n}{2}$.

(d) Let us look at all the proposed answers consecutively. We're interested in finding which ones are not constant.

- $f_1(X_1)$ — true. The string X_1 can be seen as $n-1$ random bits followed by a bit that is fully determined by the previous $n-1$ bits. Since there are $n-1$ random bits, performing $x_L \cdot x_R$ will generate a random bit. Notice that this is not uniformly random; for example, if $n = 4$, then an output of 0 is 3 times more likely than an output of 1.
- $f_1(X_2)$ — true. Since the first $\frac{n}{2}$ bits of X_2 are the same as the second half, we have $x_L \cdot x_R = XOR(x_L) = XOR(x_R)$ which is a uniformly random bit since the strings $x_L = x_R$ are random.
- $f_2(X_0)$ — true. Since the last $n-k$ bits of X_0 are fully random, the XOR of the entire string will result in a uniformly random bit.
- $f_2(X_1)$ — false. Since the number of 0's in the string is known the parity of the string (computed by the XOR) is 0 for n even.
- $f_2(X_2)$ — false. Since the first $\frac{n}{2}$ bits of X_2 are the same as the second half, the parity of the bit string is zero.

(e) The XOR of all of the bits is equal to $b \oplus r$, for r equal to the XOR of the bits learned by Eve and b equal to the XOR of all of the other bits. Regardless of the distribution of r, $b \oplus r$ is uniform independent of Eve's knowledge.

(f) $t = n - 1$. In this case there is at least one bit that Eve did not get access to. Call this bit b. From Eve's point of view, b is uniformly distributed and independent of everything else. We only require the existence of one bit that Eve does not get access to.

(g) Following the last question, each subsource must have at least $t + 1$ bits. They can make at most $\lfloor \frac{n}{t+1} \rfloor$ such subsources.