COM-440, Introduction to Quantum Cryptography, Fall 2025

Homework # 1 **due: 12:59PM, October 8th, 2019**

Ground rules:

Please format your solutions so that each problem begins on a new page, and so that your name appears at the top of each page.

You are encouraged to collaborate with your classmates on homework problems, but each person must write up the final solutions individually. You should note on your homework specifically which problems were a collaborative effort and with whom. You may not search online for solutions, but if you do use research papers or other sources in your solutions, you must cite them.

Late homework will not be accepted or graded. Extensions will not be granted, except on the recommendation of a dean. We will grade as many problems as possible, but sometimes one or two problems will not be graded. Your lowest homework grade of the semester will be dropped from your final grade.

Problems:

1. **An optimal attack**

   (a) We check that

$$N_1^\dagger N_1 + N_2^\dagger N_2 = \frac{1}{12}\begin{pmatrix}10 & 0\\ 0 & 2\end{pmatrix} + \frac{1}{12}\begin{pmatrix}2 & 0\\ 0 & 10\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\ ,$$

   as should be the case.

   (b) For example, we can compute the image of $|+\rangle$ as

$$\begin{aligned}\mathcal{N}(|+\rangle\langle+|) &= N_1\,|+\rangle\langle+|\,N_1^\dagger + N_2\,|+\rangle\langle+|\,N_2^\dagger\\ &= \frac{1}{12}\frac{1}{2}\big(3\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,\big)\big(3\,\langle 00| + \langle 01| + \langle 10| + \langle 11|\,\big)\\ &\qquad + \frac{1}{12}\frac{1}{2}\big(\,|00\rangle + |01\rangle + |10\rangle + 3\,|11\rangle\,\big)\big(\,\langle 00| + \langle 01| + \langle 10| + 3\,|11\rangle\,\big)\ .\end{aligned}$$

   We can then verify that

$$\begin{aligned}\langle+|\,\langle+|\mathcal{N}(|+\rangle\langle+|)\,|+\rangle\,|+\rangle &= \frac{1}{4}\frac{1}{24}\big((3+1+1+1)^2 + (1+1+1+3)^2\big)\\ &= \frac{1}{96}(36+36) = \frac{3}{4}\ .\end{aligned}$$

   A similar calculation gives the same for the three other BB'84 states!

2. **Secret sharing among three people.**

(a) We directly calculate one matrix and use the symmetry among A, B, C to extrapolate the others.

$$\begin{aligned}\rho_A &= \mathrm{Tr}_{BC}(|\Psi\rangle\langle\Psi|)\\ &= \frac{1}{2}(|0\rangle\langle 0|_A \otimes \mathrm{tr}(|0\rangle\langle 0|_B) \otimes \mathrm{tr}(|0\rangle\langle 0|_C) + (-1)^{2b}\,|1\rangle\langle 1|_A \otimes \mathrm{tr}(|1\rangle\langle 1|_B) \otimes \mathrm{tr}(|1\rangle\langle 1|_C))\\ &= \frac{1}{2}(|0\rangle\langle 0|_A + |1\rangle\langle 1|_A)\\ &= \frac{\mathbb{I}}{2}\end{aligned}$$

We similarly have $\rho_B = \frac{1}{2}(|0\rangle\langle 0|_B + |1\rangle\langle 1|_B) = \frac{\mathbb{I}}{2}$ and $\rho_C = \frac{1}{2}(|0\rangle\langle 0|_C + |1\rangle\langle 1|_C) = \frac{\mathbb{I}}{2}$. Notice that this state is independent of b and so any measurement these people take alone will be independent of b, and the secret cannot be retrieved on their own.

(b) Again calculate one matrix and use the symmetry among A, B, C to extrapolate the others.

$$\begin{aligned}\rho_{AB} &= \mathrm{Tr}_C(|\Psi\rangle\langle\Psi|)\\ &= \frac{1}{2}(|0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B \otimes \mathrm{tr}(|0\rangle\langle 0|_C) + (-1)^{2b}\,|1\rangle\langle 1|_A \otimes |1\rangle\langle 1|_B \otimes \mathrm{tr}(|1\rangle\langle 1|_C))\\ &= \frac{1}{2}(|0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B + |1\rangle\langle 1|_A \otimes |1\rangle\langle 1|_B)\\ &= \frac{1}{2}(|00\rangle\langle 00|_{AB} + |11\rangle\langle 11|_{AB})\end{aligned}$$

and similarly $\rho_{BC} = \frac{1}{2}(|00\rangle\langle 00|_{BC} + |11\rangle\langle 11|_{BC})$ and $\rho_{AC} = \frac{1}{2}(|00\rangle\langle 00|_{AC} + |11\rangle\langle 11|_{AC})$. Again, we see that these densities are independent of B, so any measurement made by any pair of people will not give information about b.

(c) Have Alice, Bob, and Charlie apply the Hadamard operation on their qubit to get the new state

$$|\Psi_0\rangle = \frac{1}{4}((|0\rangle + |1\rangle)^3 + (|0\rangle - |1\rangle)^3) = \frac{1}{4}((|000\rangle + |011\rangle + |110\rangle + |101\rangle))$$

if $b = 0$ and the new state

$$|\Psi_1\rangle = \frac{1}{4}((|0\rangle + |1\rangle)^3 - (|0\rangle - |1\rangle)^3) = \frac{1}{4}(|001\rangle + |010\rangle + |100\rangle + |111\rangle))$$

if $b = 1$. Next, we have Alice, Bob, and Charlie measure their qubits. Note by inspection, the tensor product of all three observations must either be in the set

$$S_0 = \{|0\rangle_A |0\rangle_B |0\rangle_C, |0\rangle_A |1\rangle_B |1\rangle_C, |1\rangle_A |1\rangle_B |0\rangle_C, |1\rangle_A |0\rangle_B |1\rangle_C\}$$

if $b = 0$, and must be in the set

$$S_1 = \{|0\rangle_A |0\rangle_B |1\rangle_C, |0\rangle_A |1\rangle_B |0\rangle_C, |1\rangle_A |0\rangle_B |0\rangle_C, |1\rangle_A |1\rangle_B |1\rangle_C\}$$

if $b = 1$.

Hence we can have Alice and Bob send their measurement to Charlie, and Charlie will see whether their collective measurements are in S_0 or S_1 to recover b.

3. **A Guessing Game.**

   (a) If we assume $U_A(|0\rangle) = \alpha_0 |0\rangle + \beta_0 |1\rangle$ and $U_A(|1\rangle) = \alpha_1 |0\rangle + \beta_1 |1\rangle$we can note that

   $$\begin{aligned}(U_A \otimes \mathbb{I}_B)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) &= \frac{1}{\sqrt{2}}(U_A(|0\rangle) \otimes |0\rangle + U_A(|1\rangle) \otimes |1\rangle) \\ &= \frac{1}{\sqrt{2}}(\alpha_0 |00\rangle + \beta_0 |10\rangle + \alpha_1 |01\rangle + \beta_1 |11\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle \otimes (\alpha_0 |0\rangle + \alpha_1 |1\rangle) + |1\rangle \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle)) \\ &= \frac{1}{\sqrt{2}}(|0\rangle \otimes U_B^T(|0\rangle) + |1\rangle \otimes U_B^T(|1\rangle)) \\ &= (\mathbb{I}_A \otimes U_B^T)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\end{aligned}$$

   Hence, if Eve applies the unitary transformation $(U^T)^{-1} = (U^\dagger)^T = U$, we will have undone this unitary transformation. Then we can replicate the argument given in the problem statement, and so using θ, can measure in the same basis that Alice did and perfectly recover Alice's bit with probability 1.

   (b) We claim that by using only two matrices unitary matrices we can get a success probability of $1/2$, which is equivalent to simply guessing. Simply have Alice choose one of $\mathbb{I}$ or H uniformly at random irregardless of θ. Then for either value of θ, the density matrix for ρ_E would be the mixture

   $$\rho_E = \frac{1}{4}(|0\rangle\langle 0| + |1\rangle\langle 1| + |+\rangle\langle +| + |-\rangle\langle -|) = \frac{\mathbb{I}}{2}$$

   which is independent of θ. Hence Eve's best bet is just guessing independently at random.

   (c) See part (b)

4. **Robustness of GHZ and W States, Part 2**

(a) By direct calculation we have

$$\mathrm{Tr}_N \left|GHZ_N\right\rangle\!\left\langle GHZ_N\right| = \frac{1}{2}\left|0\right\rangle\!\left\langle 0\right|^{\otimes N-1} + \frac{1}{2}\left|1\right\rangle\!\left\langle 1\right|^{\otimes N-1}$$

and

$$\mathrm{Tr}_N \left|W_N\right\rangle\!\left\langle W_N\right| = \frac{N-1}{N}\left|W_{N-1}\right\rangle\!\left\langle W_{N-1}\right| + \frac{1}{N}\left|0\right\rangle\!\left\langle 0\right|^{\otimes N-1} \quad .$$

Both of these are diagonal (in some basis) and have rank 2. Note that this is also the *highest* rank one can get when tracing out a single qubit, as $\rho_A = \rho_B$.

(b) For $\rho = |0\rangle\!\langle 0|$ we have $\rho^2 = \rho$ and thus $\mathrm{Tr}(\rho^2) = 1$. On the other hand, for $\rho = \frac{1}{d} id_d$ we have $\rho^2 = \frac{1}{d^2} id_d$ from which it follows that $\mathrm{Tr}(\rho^2) = \frac{1}{d}$

(c) The extremes (pure and maximally mixed) that you considered in Problem 2.2 certainly suggest this. Informally, the more entangled A and B are, the more classical uncertainty you have — the more information you lose — in the state ρ_A of A alone after tracing out B. This expresses itself as a lower purity as defined above.

(d) Again we have by direct calculation

$$\rho = \mathrm{Tr}_N \left|GHZ_N\right\rangle\!\left\langle GHZ_N\right| = \frac{1}{2}\left|0\right\rangle\!\left\langle 0\right|^{\otimes N-1} + \frac{1}{2}\left|1\right\rangle\!\left\langle 1\right|^{\otimes N-1} \quad ,$$

from which it follows that

$$\rho^2 = \frac{1}{4}\left|0\right\rangle\!\left\langle 0\right|^{\otimes N-1} + \frac{1}{4}\left|1\right\rangle\!\left\langle 1\right|^{\otimes N-1}$$

and $\mathrm{Tr}(\rho^2) = \frac{1}{2}$ for all N.

(e) We have again by direct calculation

$$\rho = \mathrm{Tr}_N \left|W_N\right\rangle\!\left\langle W_N\right| = \frac{N-1}{N}\left|W_{N-1}\right\rangle\!\left\langle W_{N-1}\right| + \frac{1}{N}\left|0\right\rangle\!\left\langle 0\right|^{\otimes N-1} \quad ,$$

from which it follows that

$$\rho^2 = \frac{(N-1)^2}{N^2}\left|W_{N-1}\right\rangle\!\left\langle W_{N-1}\right| + \frac{1}{N^2}\left|0\right\rangle\!\left\langle 0\right|^{\otimes N-1}$$

and $\mathrm{Tr}(\rho^2) = \frac{N^2-2N+2}{N^2} \to 1$ as $N \to \infty$.

As N grows, the $|GHZ_N\rangle$ states to which one qubit has been discarded have a lower purity than the $|W_N\rangle$ states. According to the preceding discussion, this means that there is more entanglement between $(N-1)$ and 1 qubits of a $|GHZ_N\rangle$ state, than there is in a $|W_N\rangle$ state. Conversely, if we consider the qubit to be "lost" then there is less entanglement remaining in the $|GHZ_N\rangle$ state. If we remove two qubits, then continuing the calculations made in 4. and 5. we see that the result is essentially unchanged.

5. **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

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

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. $\mathrm{Tr}(M\rho) \leq \mathrm{Tr}(M\sigma)$.