COM-440, Introduction to Quantum Cryptography, Fall 2025

Homework # 2 Solutions

Problems:

1. **Robustness of GHZ and W States**

   (a) First note that if $\rho = |\psi\rangle\langle\psi|$ is pure, then

   $$\mathrm{Tr}\,(\rho\sigma) = \mathrm{Tr}\,(|\psi\rangle\langle\psi|\,\sigma) = \mathrm{Tr}\,(\langle\psi|\,\sigma\,|\psi\rangle) = \langle\psi|\,\sigma\,|\psi\rangle$$

   We can view tracing out part of a state as a consequence of an unknown party, say Bob, measuring that part of the state. In this case, measuring the third qubit in the computational basis (remember that the partial trace is independent of the basis we choose, see the videos and lecture notes) gives Bob either 0 or 1 with probability a half. The corresponding states on the first two qubits are $|00\rangle\langle00|$ and $|11\rangle\langle11|$, respectively. Thus, the remaining state is $\frac{1}{2}\,|00\rangle\langle00| + \frac{1}{2}\,|11\rangle\langle11|$. We have that $|GHZ_2\rangle\langle GHZ_2| = \frac{1}{2}\,(|00\rangle\langle00| + |11\rangle\langle11| + |00\rangle\langle11| + |11\rangle\langle00|)$, which is a pure state. Using the fact that this is a pure state, we find that

   $$\begin{aligned}\mathrm{Tr}\big(\,&|GHZ_2\rangle\langle GHZ_2|\mathrm{Tr}_3\,|GHZ_3\rangle\langle GHZ_3|\,\big)\\ &= \langle GHZ_2|\,\mathrm{Tr}_3\,(|GHZ_3\rangle\langle GHZ_3|)\,|GHZ_2\rangle\\ &= \frac{1}{4}\,(\langle00|00\rangle + \langle11|11\rangle) = \frac{1}{2}\end{aligned}$$

   (b) Measuring the third qubit gives a 0 with probability $2/3$, so that the state on the other two qubits is equal to $|W_2\rangle\langle W_2|$. If a measurement on the third qubit gives a 1 (with probability $1/3$), the corresponding state on the first two qubits is $|00\rangle\langle00|$. The state on the first two qubits after tracing out the third qubit is $\mathrm{Tr}_3\,(|W_3\rangle\langle W_3|) = \frac{2}{3}\,|W_2\rangle\langle W_2| + \frac{1}{3}\,|00\rangle\langle00|$. Since $\langle W_2|00\rangle = 0$, we have that

   $$\mathrm{Tr}\,(|W_2\rangle\langle W_2|\,\mathrm{Tr}_3\,(|W_3\rangle\langle W_3|)) = \frac{2}{3}$$

   (c) We have that

   $$\mathrm{Tr}_N\,(|GHZ_N\rangle\langle GHZ_N|) = \frac{1}{2}|\underbrace{00\ldots0}_{N-1}\rangle\langle\underbrace{00\ldots0}_{N-1}| + \frac{1}{2}|\underbrace{11\ldots1}_{N-1}\rangle\langle\underbrace{11\ldots1}_{N-1}|$$

   Using similar reasoning as in the first problem, we find that the overlap is equal to $1/2$.

(d) Measuring the last qubit gives a 0 with probability $\frac{N-1}{N}$, so that the state on the remaining qubits is equal to $|W_{N-1}\rangle\langle W_{N-1}|$. If a measurement on the last qubit gives a 1 (with probability $\frac{1}{N}$), the corresponding state on the remaining qubits is $|\underbrace{00\ldots0}_{N-1}\rangle\langle\underbrace{00\ldots0}_{N-1}|$. The state on the first $N-1$ qubits after tracing out the last qubit is then $\mathrm{Tr}_N\left(|W_N\rangle\langle W_N|\right) = \frac{N-1}{N}|W_{N-1}\rangle\langle W_{N-1}| + \frac{1}{N}|\underbrace{00\ldots0}_{N-1}\rangle\langle\underbrace{00\ldots0}_{N-1}|$. Since $\langle W_{N-1}|\underbrace{00\ldots}_{N-1}\rangle = 0$, we have that $\mathrm{Tr}\Big(|W_{N-1}\rangle\langle W_{N-1}|\,\mathrm{Tr}_N\left(|W_N\rangle\langle W_N|\right)\Big) = \frac{N-1}{N}$. Taking the limit we get $\lim_{N\to\infty}\frac{N-1}{N} = 1$.

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

(a) By direct calculation we have

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

and

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

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

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

from which it follows that

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

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

(e) We have again by direct calculation

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

from which it follows that

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

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.