COM-440, Introduction to Quantum Cryptography, Fall 2025

Homework # 2 **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. (4 points) **The EPR pair.** Recall the definition of the EPR pair,

$$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\,\big)\ .$$

   Prove rigorously that there does not exist two single-qubit states $|\psi\rangle$ and $|\phi\rangle$ such that $|\mathrm{EPR}\rangle = |\psi\rangle \otimes |\phi\rangle$. *[Hint: Reason by contradiction. Expand everything in the standard basis.]*

2. **Robustness of GHZ and W States**
   In this problem we explore two classes of N-qubit states that are especially useful for cryptography and communication, but behave very differently under tracing out a single qubit. Let's first define them for $N = 3$:

$$\text{GHZ state:} \quad |GHZ_3\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

$$\text{W state:} \quad |W_3\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)$$

   Note that both states are symmetric under permutation of the three qubits, so without loss of generality we may trace out the last one, Tr_3. Also, we have analogously $|GHZ_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $|W_2\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$.

   In the following we consider the *overlap* between N-qubit GHZ and W states with one qubit discarded (i.e. traced out) and their $(N-1)$-qubit counterparts. The overlap of density matrices ρ and σ is defined as $\mathrm{Tr}\rho\sigma$, a measure of "closeness" that generalizes the expression $|\langle\phi|\psi\rangle|^2$ for pure states.

(a) Calculate the overlap between $|GHZ_2\rangle\langle GHZ_2|$ and $\mathrm{Tr}_3\,|GHZ_3\rangle\langle GHZ_3|$.

(b) Calculate the overlap between $|W_2\rangle\langle W_2|$ and $\mathrm{Tr}_3\,|W_3\rangle\langle W_3|)$.

Now we generalize to the N-qubit case. As you might expect, $|GHZ_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N})$ and $|W_N\rangle$ is an equal superposition of all N-bit strings with exactly one 1 and $N-1$ 0's.

3. What is the overlap $\mathrm{Tr}(|GHZ_{N-1}\rangle\langle GHZ_{N-1}|\,\mathrm{Tr}_N\,|GHZ_N\rangle\langle GHZ_N|)$ in the limit $N \to \infty$?
4. What is the overlap $\mathrm{Tr}(|W_{N-1}\rangle\langle W_{N-1}|\,\mathrm{Tr}_N\,|W_N\rangle\langle W_N|)$ in the limit $N \to \infty$?

The interpretation of these results is that W states are more "robust" against loss of a single qubit than GHZ states.

3. **Robustness of GHZ and W States, Part 2**
We return to the multi-qubit GHZ and W states introduced in the previous exercise. In class we learned to distinguish product states from (pure) entangled states by calculating the Schmidt rank of $|\Psi\rangle_{AB}$, i.e. the rank of the reduced state $\rho_A = \mathrm{Tr}_B\,|\Psi\rangle\langle\Psi|$. In particular ρ is pure if and only if $|\Psi\rangle$ has Schmidt rank 1. In the following, we denote by Tr_N the operation of tracing out only the last of N qubits.

(a) What are the ranks r_{GHZ} of $\mathrm{Tr}_N\,|GHZ_N\rangle\langle GHZ_N|$ and r_W of $\mathrm{Tr}_N\,|W_N\rangle\langle W_N|$, respectively? (Note that these are the Schmidt ranks of $|GHZ_N\rangle$ and $|W_N\rangle$ if we partition each of them between the first $N-1$ qubits and the last qubit.)

Let us now introduce a more discriminating (in fact, continuous) measure of the entanglement of a state $|\Psi\rangle_{AB}$: namely, the *purity* of the reduced state ρ_A given by $\mathrm{Tr}\rho_A^2$. First let's see how this works in practice with the extreme cases in d dimensions:

2. What are the purities $\mathrm{Tr}\,(\rho^2)$ for $\rho = |0\rangle\langle 0|$ and the "maximally mixed" state $\rho = \frac{1}{d}id_d$, respectively?
3. Is the purity of ρ_A higher or lower for more entangled states $|\Psi\rangle_{AB}$? Can you explain this in terms of the definition $\mathrm{Tr}\,(\rho_A^2)$?

Now consider again the behavior of the N-qubit GHZ and W states with one qubit discarded (i.e. traced out):

4. What is the purity of $\mathrm{Tr}_N\,|GHZ_N\rangle\langle GHZ_N|$ in the limit $N \to \infty$?
5. What is the purity of $\mathrm{Tr}_N\,|W_N\rangle\langle W_N|$ in the limit $N \to \infty$?

Discuss the implications for the "robustness" of multipartite entanglement under loss of one qubit in GHZ versus W states. What can we say about losses of more than one qubit?