Math 4981 Spring 2021
Cryptography HW 10
Due Thursday, April 1

1. What do each of the functions $\mathbf{n}^2, \overline{\mathbf{n}}^2, \mathbf{n}\overline{\mathbf{n}}$, and $\mathbf{nX}$ do to $|0\rangle$ and $|1\rangle$? Can you express these functions in terms of functions we have already named?

2. Consider the swap operator $\mathbf{S}$ on two bits, defined by the formula

$$\mathbf{S} = \mathbf{n} \otimes \mathbf{n} + \overline{\mathbf{n}} \otimes \overline{\mathbf{n}} + (\mathbf{X} \otimes \mathbf{X})(\mathbf{n} \otimes \overline{\mathbf{n}}) + (\mathbf{X} \otimes \mathbf{X})(\overline{\mathbf{n}} \otimes \mathbf{n}).$$

   (a) Prove that $\mathbf{S}^2 = \mathbf{1}$ using this algebraic definition and the relations we have for $\mathbf{n}, \mathbf{X}$, and $\mathbf{1}$.

   (b) Check that $\mathbf{S}$ does in fact swap two bits by computing its output for each possible two-bit input.

   (c) Write down a matrix representation of $\mathbf{S}$. (This should be a 4×4 matrix.

3. Prove that $\mathbf{HXH} = \mathbf{Z}$ and $\mathbf{HZH} = \mathbf{X}$.

4. Let A be a $m \times n$ matrix, and let $\psi \in \mathbb{C}^n, \phi \in \mathbb{C}^m$. If $A^\dagger$ is the conjugate transpose of A, prove that $\langle A^\dagger \phi | \psi \rangle = \langle \phi | A\psi \rangle$. (That is, prove the conjugate transpose is in fact the adjoint of A.)

   (Note: this is slightly different from the definition of adjoint I gave in the notes; but it's equivalent because $(A^\dagger)^\dagger = A$.)

5. If U is a $n \times n$ unitary matrix, prove that $\langle U\psi | U\phi \rangle = \langle \psi | \phi \rangle$ for any vectors $\psi, \phi \in \mathbb{C}^n$.

6. In this problem we'll show that a very simple hidden-variable theory can't explain the Born rule. A common misconception is that a qubit is "really" either in the state $|0\rangle$ or $|1\rangle$, and when we measure it we find out which. But this is inconsistent with the results of calculations we can do; measuring the state of a qubit really does change its state.

   Let $|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

   (a) What is $\mathbf{H}(|\phi\rangle)$?

   (b) If we measure $\mathbf{H}(|\phi\rangle)$, what is the probability of each possible outcome?

   (c) If we measure $|\phi\rangle$, what is the probability of each possible outcome?

   (d) Suppose we measure $|\phi\rangle$ and get $|0\rangle$ as our outcome. What happens if we now apply $\mathbf{H}$? What is the result of taking a measurement?

   (e) Repeat part (d) in the case where we get $|1\rangle$ as our outcome?