Math 4981 Spring 2021
Cryptography HW 10 Solutions
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?

   Solution: We have

$$\begin{array}{lll}
\mathbf{nn}|0\rangle = \mathbf{n}\vec{0} = \vec{0} & \mathbf{nn}|1\rangle = \mathbf{n}|1\rangle = |1\rangle & \mathbf{nn} = \mathbf{n} \\
\overline{\mathbf{nn}}|0\rangle = \overline{\mathbf{n}}|0\rangle = |0\rangle & \overline{\mathbf{nn}}|1\rangle = \overline{\mathbf{n}}\vec{0} = \vec{0} & \overline{\mathbf{n}}^2 = \overline{\mathbf{n}} \\
\mathbf{n}\overline{\mathbf{n}}|0\rangle = \mathbf{n}|0\rangle = \vec{0} & \mathbf{n}\overline{\mathbf{n}}|1\rangle = \mathbf{n}\vec{0} = \vec{0} & \mathbf{n}\overline{\mathbf{n}} = \mathbf{0} \\
\mathbf{nX}|0\rangle = \mathbf{n}|1\rangle = |1\rangle & \mathbf{nX}|1\rangle = \mathbf{n}|0\rangle = \vec{0} & \\
\mathbf{X}\overline{\mathbf{n}}|0\rangle = \mathbf{X}|0\rangle = |1\rangle & \mathbf{X}\overline{\mathbf{n}}|1\rangle = \mathbf{X}\vec{0} = \vec{0} & \mathbf{nX} = \mathbf{X}\overline{\mathbf{n}}.
\end{array}$$

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 $\mathbf{1}$.

Solution:

$$
\begin{aligned}
\mathbf{S}^2 &= \mathbf{n}\otimes\mathbf{n}\big(\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})\big)\\
&\quad+\overline{\mathbf{n}}\otimes\overline{\mathbf{n}}\big(\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})\big)\\
&\quad+(\mathbf{X}\otimes\mathbf{X})(\mathbf{n}\otimes\overline{\mathbf{n}})\big(\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})\big)\\
&\quad+(\mathbf{X}\otimes\mathbf{X})(\overline{\mathbf{n}}\otimes\mathbf{n})\big(\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})\big)\\
&= \mathbf{n}^2\otimes\mathbf{n}^2+\mathbf{n}\overline{\mathbf{n}}\otimes\mathbf{n}\overline{\mathbf{n}}+\mathbf{n}\mathbf{X}\mathbf{n}\otimes\mathbf{n}\mathbf{X}\overline{\mathbf{n}}+\mathbf{n}\mathbf{X}\overline{\mathbf{n}}\otimes\mathbf{n}\mathbf{X}\mathbf{n}\\
&\quad+\overline{\mathbf{n}}\mathbf{n}\otimes\overline{\mathbf{n}}\mathbf{n}+\overline{\mathbf{n}}^2\otimes\overline{\mathbf{n}}^2+\overline{\mathbf{n}}\mathbf{X}\mathbf{n}\otimes\overline{\mathbf{n}}\mathbf{X}\overline{\mathbf{n}}+\overline{\mathbf{n}}\mathbf{X}\overline{\mathbf{n}}\otimes\overline{\mathbf{n}}\mathbf{X}\mathbf{n}\\
&\quad+\mathbf{X}\mathbf{n}^2\otimes\mathbf{n}\overline{\mathbf{n}}\mathbf{n}+\mathbf{X}\mathbf{n}\overline{\mathbf{n}}\otimes\mathbf{X}\overline{\mathbf{n}}^2+\mathbf{X}\mathbf{n}\mathbf{X}\mathbf{n}\otimes\mathbf{X}\overline{\mathbf{n}}\mathbf{X}\overline{\mathbf{n}}+\mathbf{X}\mathbf{n}\mathbf{X}\overline{\mathbf{n}}\otimes\mathbf{X}\overline{\mathbf{n}}\mathbf{X}\mathbf{n}\\
&\quad+\mathbf{X}\overline{\mathbf{n}}\mathbf{n}\otimes\mathbf{X}\mathbf{n}^2+\mathbf{X}\overline{\mathbf{n}}^2\otimes\mathbf{X}\mathbf{n}\overline{\mathbf{n}}+\mathbf{X}\overline{\mathbf{n}}\mathbf{X}\mathbf{n}\otimes\mathbf{X}\mathbf{n}\mathbf{X}\overline{\mathbf{n}}+\mathbf{X}\overline{\mathbf{n}}\mathbf{X}\overline{\mathbf{n}}\otimes\mathbf{X}\mathbf{n}\mathbf{X}\mathbf{n}\\
&= \mathbf{n}\otimes\mathbf{n}+\mathbf{0}\otimes\mathbf{0}+\mathbf{X}\overline{\mathbf{n}}\mathbf{n}\otimes\mathbf{X}\overline{\mathbf{n}}^2+\mathbf{X}\overline{\mathbf{n}}^2\otimes\mathbf{X}\overline{\mathbf{n}}\mathbf{n}\\
&\quad+\mathbf{0}\otimes\mathbf{0}+\overline{\mathbf{n}}\otimes\overline{\mathbf{n}}+\mathbf{X}\mathbf{n}^2\otimes\mathbf{X}\mathbf{n}\overline{\mathbf{n}}+\mathbf{X}\mathbf{n}\overline{\mathbf{n}}\otimes\mathbf{X}\mathbf{n}^2\\
&\quad+\mathbf{X}\mathbf{n}\otimes\mathbf{0}\mathbf{n}+\mathbf{X}\mathbf{0}\otimes\mathbf{X}\overline{\mathbf{n}}+\mathbf{X}^2\overline{\mathbf{n}}\mathbf{n}\otimes\mathbf{X}^2\mathbf{n}\overline{\mathbf{n}}+\mathbf{X}^2\overline{\mathbf{n}}^2\otimes\mathbf{X}^2\mathbf{n}^2\\
&\quad+\mathbf{X}\mathbf{0}\otimes\mathbf{X}\mathbf{n}+\mathbf{X}\overline{\mathbf{n}}\otimes\mathbf{X}\mathbf{0}+\mathbf{X}^2\mathbf{n}^2\otimes\mathbf{X}^2\overline{\mathbf{n}}^2+\mathbf{X}^2\mathbf{n}\overline{\mathbf{n}}\otimes\mathbf{X}^2\overline{\mathbf{n}}\mathbf{n}\\
&= \mathbf{n}\otimes\mathbf{n}+\mathbf{0}\otimes\mathbf{0}+\mathbf{0}\otimes\mathbf{X}\overline{\mathbf{n}}+\mathbf{X}\overline{\mathbf{n}}\otimes\mathbf{0}\\
&\quad+\mathbf{0}\otimes\mathbf{0}+\overline{\mathbf{n}}\otimes\overline{\mathbf{n}}+\mathbf{X}\mathbf{n}\otimes\mathbf{0}+\mathbf{0}\otimes\mathbf{X}\mathbf{n}\\
&\quad+\mathbf{X}\mathbf{n}\otimes\mathbf{0}+\mathbf{0}\otimes\mathbf{X}\overline{\mathbf{n}}+\mathbf{0}\otimes\mathbf{0}+\overline{\mathbf{n}}\otimes\mathbf{n}\\
&\quad\mathbf{0}\otimes\mathbf{X}\mathbf{n}+\mathbf{X}\overline{\mathbf{n}}\otimes\mathbf{0}+\mathbf{n}\otimes\overline{\mathbf{n}}+\mathbf{0}\otimes\mathbf{0}\\
&= \mathbf{n}\otimes\mathbf{n}+\overline{\mathbf{n}}\otimes\overline{\mathbf{n}}+\overline{\mathbf{n}}\otimes\mathbf{n}+\mathbf{n}\otimes\overline{\mathbf{n}}\\
&= \mathbf{n}\otimes(\mathbf{n}+\overline{\mathbf{n}})+\overline{\mathbf{n}}\otimes(\mathbf{n}+\overline{\mathbf{n}})=\mathbf{n}\otimes\mathbf{1}+\overline{\mathbf{n}}\otimes\mathbf{1}\\
&= (\mathbf{n}+\overline{\mathbf{n}})\otimes\mathbf{1}=\mathbf{1}\otimes\mathbf{1}.
\end{aligned}
$$

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

Solution:

$$
\begin{aligned}
\mathbf{S}|00\rangle &= \vec{0}\otimes\vec{0}+|0\rangle\otimes|0\rangle+\mathbf{X}(\vec{0})\otimes\mathbf{X}(|0\rangle)+\mathbf{X}(|0\rangle)\otimes\mathbf{X}(\vec{0})\\
&= \vec{0}\otimes\vec{0}+|0\rangle\otimes|0\rangle+\vec{0}\otimes|1\rangle+|1\rangle\otimes\vec{0}\\
&= \vec{0}+|00\rangle+\vec{0}+\vec{0}=|00\rangle\\
S|01\rangle &= \vec{0}\otimes|1\rangle+|0\rangle\otimes\vec{0}+\vec{0}\otimes\vec{0}+|1\rangle\otimes|0\rangle=|10\rangle\\
S|10\rangle &= |1\rangle\otimes\vec{0}+\vec{0}\otimes|0\rangle+|0\rangle\otimes|1\rangle+\vec{0}\otimes\vec{0}=|01\rangle\\
S|11\rangle &= |1\rangle\otimes|1\rangle+\vec{0}\otimes\vec{0}+|0\rangle\otimes\vec{0}+\vec{0}\otimes|0\rangle=|11\rangle.
\end{aligned}
$$

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

Solution:

$$
\begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}
$$

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

Solution: We can take two basic approaches: checking outputs on bits, or using matrices. On bits:

$$\begin{aligned}
\mathbf{HXH}|0\rangle &= \frac{1}{\sqrt{2}}\mathbf{HX}(|0\rangle + |1\rangle) \\
&= \frac{1}{\sqrt{2}}\mathbf{H}(|1\rangle + |0\rangle) \\
&= \frac{1}{2}\left(|0\rangle - |1\rangle + |0\rangle + |1\rangle\right) = |0\rangle = \mathbf{Z}|0\rangle \\
\mathbf{HXH}|1\rangle &= \frac{1}{\sqrt{2}}\mathbf{HX}(|0\rangle - |1\rangle) \\
&= \frac{1}{\sqrt{2}}\mathbf{H}(|1\rangle - |0\rangle) \\
&= \frac{1}{2}(|0\rangle - |1\rangle - (|0\rangle + |1\rangle) = -|1\rangle = \mathbf{Z}|1\rangle \\
\mathbf{HZH}|0\rangle &= \frac{1}{\sqrt{2}}\mathbf{HZ}(|0\rangle + |1\rangle) \\
&= \frac{1}{\sqrt{2}}\mathbf{H}(|0\rangle - |1\rangle) \\
&= \frac{1}{2}(|0\rangle + |1\rangle - (|0\rangle - |1\rangle) = |1\rangle = \mathbf{X}|0\rangle \\
\mathbf{HZH}|1\rangle &= \frac{1}{\sqrt{2}}\mathbf{HZ}(|0\rangle - |1\rangle) \\
&= \frac{1}{\sqrt{2}}\mathbf{H}(|0\rangle + |1\rangle) \\
&= \frac{1}{2}(|0\rangle + |1\rangle + (|0\rangle - |1\rangle) = |0\rangle = \mathbf{X}|1\rangle.
\end{aligned}$$

We could also use matrices. We know that $\mathbf{H}$ corresponds to $\frac{1}{\sqrt{2}}\left[\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right]$, $\mathbf{Z}$ to $\left[\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right]$, and $\mathbf{X}$ to $\left[\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right]$. Then

$$\begin{aligned}
\mathbf{HXH} &= \frac{1}{2}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \\
&= \frac{1}{2}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}2 & 0\\ 0 & -2\end{bmatrix} \\
\mathbf{HZH} &= \frac{1}{2}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \\
&= \frac{1}{2}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1 & 1\\ -1 & 1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}0 & 2\\ 2 & 0\end{bmatrix}.
\end{aligned}$$

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 $(A^\dagger)^\dagger = A$.)

Solution: If $\vec{u}, \vec{v}$ are column vectors, then $\langle u|v\rangle = \vec{v}^\dagger \vec{u}$. Thus we have

$$\langle A^\dagger \phi|\psi\rangle = \psi^\dagger A^\dagger \phi = (A\psi)^\dagger \phi = \langle \phi|A\psi\rangle.$$

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 $\psi, \phi \in \mathbb{C}^n$.

   Solution: By adjointness, we have

$$\langle U\psi|U\phi\rangle = \langle \psi|U^\dagger U\phi\rangle = \langle \psi|I\phi\rangle = \langle \psi|\phi\rangle.$$

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?

   Solution:

   (a)
$$\mathbf{H}|\phi\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |0\rangle - |1\rangle) = |0\rangle.$$

   (b) When we measure $\mathbf{H}|\phi\rangle$, then $p(|0\rangle)1$ and $p(|1\rangle) = 0$.

   (c) If we measure $|\phi\rangle$, we have $p(|0\rangle) = p(|1\rangle) = 1/2$.

   (d) If we measure $|\phi\rangle$ and get $|0\rangle$, our qubit is now in the state $|0\rangle$. We apply $\mathbf{H}$ and get $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Then the probability of each measurement outcome is $1/2$.

   (e) If we measure $|\phi\rangle$ and get $|1\rangle$, then the state is $|1\rangle$, so after we apply $\mathbf{H}$ we get $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Then the probability of each measurement outcome is $1/2$.