CS333 - Problem Set 1

1. Read over the Syllabus. (You don't need to follow links - you can go back to them later as needed.) Then go to the Syllabus Discussion Channel on Teams, and post a comment or a question or respond to an existing post by replying. If someone has already posted your question or comment, you can give it a thumbs-up.

2. In your personal section of OneNote, under the Reflection section, you should find the Page "Advice from Last Year's Students." Please read over their advice, and add your own response on the page, either following the prompt, or based on what is meaningful to you. (This page is only visible to you and to me, not to other students.)

3. Consider a message m that consists of one bit, so $m \in \{0, 1\}$, and a secret key $s \in \{0, 1\}$. Using the XOR encryption from class, create a table that shows what $\overline{m}$ is for every possible message/key combination. Use this table to argue that secret key encryption is very secure, as Eve can not determine m from $\overline{m}$ if she knows nothing about the value of m or s. (You may also use Baye's rule, if you know it, but this is not necessary.)

4. Do the Math Practice and then check your answers/approaches with the Solutions. If you want additional resources to learn about complex numbers and linear algebra, see the course website. If you have questions about any of this material, please come discuss with me, or with the tutors, or with your classmates. As you saw in the advice, this math is the basis upon which we are going to be building our understanding of quantum computing. We will continue to get more practice with this throughout the semester, but practicing and working to understand now will help you later!

5. Let $\mathbf{v_1} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\mathbf{v_2} = \begin{pmatrix} 0 \\ i \end{pmatrix}$, $\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$,

   (a) Calculate
   $$\left|(\mathbf{v_2} \otimes \mathbf{v_1})^\dagger \cdot (\mathbf{H} \otimes \mathbf{I}) \cdot (\mathbf{v_1} \otimes \mathbf{v_1})\right|^2. \tag{1}$$
   but do it WITHOUT multiplying out any tensor products. Instead, use the tensor product properties from the Math Practice.

   (b) While this expression looks like a bunch of random matrix multiplication, if we interpret it as a quantum system, it corresponds to taking two quantum coins that are both initially heads, randomly flipping the first one, and then determining the probability that the first coin is a tails and the second is a head. With this interpretation, is the end result the same as what you would expect with classical coins? Please comment.

6. As mentioned in the Math Practice, normalized vectors are vectors $\mathbf{v}$ such that $\mathbf{v}^\dagger \mathbf{v} = 1$. If we have a vector that is not normalized, then we can normalize it by multiplying it by a real

number α to get $\mathbf{v}' = \alpha\mathbf{v}$ where $\mathbf{v}'$ is normalized. We say $\mathbf{v}'$ is the normalized version of $\mathbf{v}$. What is the normalized version of $\mathbf{v} = \begin{pmatrix} 1 \\ e^{iw} \end{pmatrix}$, and what value of α is used to normalize it? (While this perhaps seems like cheating, to just multiply a vector by something to get it to do what we want, it is something that comes up when analyzing quantum systems.)