...I am realistic enough to know that life is a complex matter.
– Walt Disney

Problem Set 2

PCMI USS, Summer 2023

1. (a) Write the matrix form in the computational basis (yellow noation) of the operator $A = |-\rangle\langle-|$.

   (b) Consider the state $|\psi\rangle = |1\rangle$. What is the result when the operator A is applied to $|\psi\rangle$? Compute this in two different ways: (i) multiply a yellow matrix times a yellow vector; (ii) use Dirac notation. Check that your answers are the same. Which notation do you prefer? Which notation does your neighbor prefer? Which notation do your lecturer and TA prefer?

   (c) Describe the operator A geometrically. Then explain your answer to (b) geometrically.

   (d) What familiar operator is $|0\rangle\langle 0| + |1\rangle\langle 1|$? How about $|0\rangle\langle 0| - |1\rangle\langle 1|$? Can you find a similar-looking expression for the quantum NOT operator X?

   (e) Write the matrix form in the computational basis of the operator $B = |+\rangle\langle+| + |-\rangle\langle-|$

   (f) You should have gotten a nice answer to (e). Generalize. Prove.

2. **(The Pauli operators)** The four single-qubit operators $\{I, X, Y, Z\}$ are called the **Pauli operators**. Here I is the 2×2 identity matrix, and we have already met X and Z. The remaining operator Y is defined by

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

   (a) Express Y in outer product notation (similar to the expressions you found for I,X,Z.)

   (b) Which of the Pauli matrices are unitary? Which are Hermitian?

   (c) For each Pauli matrix find its eigenvalues and eigenvectors.

   (d) Any other reasons to like the Pauli matrices?

3. An important class of operator are the **positive operators**.

   Definition 1 *An operator* $A : V \to V$ *is called* **positive** *if* $\langle v|A|v\rangle \geq 0$ *for all* $v \in V$. *We say* A *is* **positive definite** *if* $\langle v|A|v\rangle > 0$ *for all* $v \in V$.

   Prove that if A is any operator, then $A^\dagger A$ is a positive operator.

4. It turns out

   Theorem 2 *Every positive operators is Hermitian.*

   Prove the theorem using the following outline.

   (a) Let $|v\rangle \in V$. Show that if $\langle w|v\rangle = 0$ for all $|w\rangle \in V$, then $|v\rangle = 0$.

   (b) Let A be a linear operator on V. Show that if $\langle w|A|v\rangle = 0$ for all $|v\rangle$ and $|w\rangle$ in V, then $A = 0$.

   (c) Let A be a linear operator on V. Show that if $\langle v|A|v\rangle = 0$ for all $|v\rangle \in V$, then $A = 0$. [Hint: Expand $\langle v + w|A|v + w\rangle$ and $\langle v + iw|A|v + iw\rangle$.]

   (d) Take a break by showing that the conclusion of part (c) is not true for *real* inner product spaces.

   (e) Now complete the proof of the theorem. [Hint: Assume that M is a positive operator, and apply part (c) to the operator $A = M - M^\dagger$.]

   (f) Explain how the theorem implies that if A is a positive operator, then there is a basis in which the matrix of A is diagonal with nonnegative real entries on the diagonal.

   (g) What can you say if A is positive definite?

5. In $BB84$, suppose there is an eavesdropper Eve who randomly chooses between the computational basis and the Hadamard basis, and uses that basis to measure a single one of the qubits $|\psi_i\rangle$ that Alice sends. Eve then sends the collapsed qubit on to Bob. Analyse the possibilities for how this plays out. With what probability can Eve correctly guess the ith bit of Alice's key? What is the probability that Eve's tampering will be detected? What if Eve does this with s qubits instead of just 1?

6. **(The B92 Key Exchange Protocol)** (adapted from Rieffel and Polak, *Quantum Computing: A Gentle Introduction*)

   As an alternative to BB84, in 1992 Bennett proposed the following. Alice chooses a random bitstring x. Let x_i be the ith bit of Alice's string. If $x_i = 0$, Alice creates the state $|\psi_i\rangle = |0\rangle$; if $x_i = 1$, Alice creates the state $|\psi_i\rangle = |+\rangle$. Alice then sends all the $|\psi_i\rangle$ to Bob. At that point, Bob generates random bits y_i. If $y_i = 0$, Bob measures $|\psi_i\rangle$ in the standard basis, and otherwise Bob measures $|\psi_i\rangle$ in the Hadamard basis $\{|+\rangle, |-\rangle\}$ (or equivalently, performs a Hadamard first before measuring). If Bob measures a $|0\rangle$ or $|+\rangle$, Bob sends a (classical) 0 to Alice; otherwise, if Bob measures a $|1\rangle$ or $|-\rangle$, Bob sends a 1. Alice and Bob then discard all bits for which Bob's bit value was 0. Let x' and y' be the resulting strings.

   (a) Show that at this point (if everything went smoothly and there was no eavesdropping), x' and y' are identical strings. Why did Alice and Bob decide to discard the bits when Bob's bit was a 0?

(b) At this point, like in BB84, Alice and Bob compare half of the bits of x' and y' to detect tampering. The remaining bits of x' and y' are the shared key. How good does this protocol seem? Does it protect against eavesdropping? In particular, suppose that Eve intercepts $|\psi_i\rangle$ and measures it in either the computational basis or the Hadamard basis and then forwards the measured qubits to Bob. On average, what percentage of Alice and Bob's key does Eve know for sure after listening in on Alice and Bob's classical communication? If Alice and Bob compare s bits of their string, what is the probability that they will detect Eve's presence?