Week 12 Exercises (ECE 598 DA)

Exercise (Measuring a Qubit in Superposition): A qubit is in the state $|\psi\rangle = \frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle$.

1. What is the probability of obtaining outcome $|0\rangle$ versus $|1\rangle$ if this qubit is measured in the $\{|0\rangle, |1\rangle\}$ computational basis?

2. After the measurement, assuming the outcome $|0\rangle$ is observed, what state does the qubit collapse into? What if the outcome $|1\rangle$ is observed?

3. Verify that $|\psi\rangle$ is a normalized state.

Exercise (Eavesdropping in BB84 Error Rate Analysis): In the BB84 protocol, suppose an eavesdropper Eve intercepts each qubit sent by Alice, measures it in a random basis (independently choosing Z or X for each qubit), and then forwards a new photon to Bob prepared in the state corresponding to her measurement result. This is the simplest "intercept-resend" attack. Assuming Alice and Bob are using the standard BB84 with Z and X bases chosen at random:

1. What fraction of qubits sent by Alice does Eve measure in the *wrong* basis (i.e., a basis different from the one Alice used for that qubit)?

2. For those qubits where Eve used the wrong basis, what is the probability that Bob's measurement (in the correct basis, which matches Alice's) will disagree with Alice's original bit value?

3. Overall, what error rate (quantum bit error rate) will Alice and Bob observe in the sifted key if Eve performs this intercept-resend attack on all qubits?

Exercise (Factoring a Small Number with Shor's Algorithm): To better understand Shor's algorithm, let's apply its logic to factor the number $N = 15$.

1. Pick a random a between 2 and 14. (If a shares a common factor with 15, we are already done. Suppose we pick $a = 2$, which is coprime to 15.)

2. What is the order r of $a = 2$ modulo 15? In other words, find the smallest $r > 0$ such that $2^r \equiv 1 \pmod{15}$.

3. Using the found r, explain how to derive a factor of 15.

4. Verify the factorization of 15.