Quantum Computing Exercises, November 24, 2000

1. Suppose Alice and Bob want to establish $n = 3$ shared random bits using the BB84 protocol for quantum key distribution (Nielsen-Chuang p.588). Take $\delta = 0$ for simplicity. In step 1 Alice selects the random string

   $$011010100100$$

   and in step 2 she selects the random bases

   $$101010101101$$

   Here 0 is the basis $\{|0\rangle, |1\rangle\}$ and 1 is the basis $\{|+\rangle, |-\rangle\}$.

   (a) What 12-qubit state does Alice send to Bob in step 3?

   (b) Suppose Eve measures the 6th and 12th qubit in the computational basis and sees a $|0\rangle$ for the 6th and a $|1\rangle$ for the 12th. In step 4, Bob measures according to the random bases

   $$110110001011$$

   Give a possible measurement outcome for him.

   (c) In step 6 Alice and Bob discard the bits for which they measured in different bases. Which bits are these?

   (d) In step 7, Alice selects bits 1,5,12. In step 8, Alice and Bob compare the values they measured for those three bits. How can they see that Eve looked at the initial qubits?

2. Consider the 1-qubit error given by

   $$E = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

   Write this matrix as a linear combination of identity (I), bit-flip (X), phase-flip (Z), and bit-flip+phase-flip (Y).

3. Consider the encoding of $|1\rangle$ in Shor's 9-qubit code:

   $$|1\rangle_L = \frac{1}{\sqrt{8}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle).$$

   (a) See what happens to the state $|1\rangle_L$ if the above 1-qubit error E is applied to the first qubit, and how the correction of this error works.

   (b) In the 9-qubit code we know how to correct a single qubit error. Suppose the probability of a single error is 0.001. What is the probability that there are more than 1 errors on those 9 qubits?