CMSC491 Introduction to Quantum Computation, VCU
Fall 2015, Assignment 9

Due: Tuesday, December 3 at start of class

Total marks: 20 marks + 10% bonus for typing your solutions in LaTeX.

1 Exercises

1. (10 marks) This question gets you to think about CSS codes.

   (a) (2 marks) Prove that for any linear code C, the distance of the code is the minimum Hamming weight of any string $x \in C$.

   (b) (2 marks) Let G and K be the generator and parity check matrices for a linear code C. Prove that $KG = 0$.

   (c) (6 marks) In class we showed how to construct a CSS code with codewords

   $$\sum_{j=0}^{N-1} \alpha_j |x_j + C_2\rangle.$$

   Suppose now that we apply an error corresponding to Pauli Y to qubit 1 of this codeword. Show how the error-correcting procedure for CSS codes corrects this error. In other words, run through an analysis similar to page 7 of the notes titled "Lecture 17: General quantum errors; CSS codes".

2. (10 marks) This question gets you to think about quantum key distribution.

   (a) (1 mark) Suppose Alice wishes to use the one-time pad to send an encrypted string $x = 01101$ to Bob. Suppose further that Alice and Bob share a secret key $k = 11011$. What is the encoded ciphertext which Alice sends to Bob in the one-time pad scheme?

   (b) (1 marks) Quantum key distribution (QKD) is a scheme for Alice and Bob to establish a joint shared secret key. In the QKD scheme, suppose Alice begins by preparing state

   $$|\psi\rangle = |+\rangle|-\rangle|0\rangle|1\rangle|1\rangle|-\rangle$$

   which she will then send to Bob. What is the secret string encoded by the state above?

   (c) (6 marks) Suppose that upon receiving $|\psi\rangle$, Bob measures the first three qubits in the correct bases, and the last three qubits in the wrong bases. There are 8 possible binary strings $x \in \{0,1\}^6$ which Bob may receive as a result of these measurements. What are these 8 strings? What is the probability of obtaining each of these strings? Which qubits of $|\psi\rangle$ do Alice and Bob discard after this measurement, and which do they keep?

   (d) (2 marks) Suppose now that Eve had intercepted $|\psi\rangle$ on its way from Alice to Bob, and measured qubit 1 in the standard basis. She then sent all the qubits on to Bob, who was oblivious to Eve's actions. What is the probability that Alice and Bob detected Eve's tampering? (Hint: To detect Eve's tampering, Bob must measure qubit 1 in the correct basis which Alice used to prepare qubit 1, but nevertheless obtain the *wrong* measurement outcome relative to how Alice originally prepared qubit 1.)