# Problem Set #1

Quantum Error Correction
Instructor: Daniel Gottesman

Due Thursday, May 26, 2016

**Problem #1. Unitary decoder**

Suppose $\mathcal{H}_N = \mathcal{H}_A \otimes \mathcal{H}_B$, with $\mathcal{H}_B = \mathcal{H}_K$ the logical Hilbert space and $\mathcal{H}_N$ the physical Hilbert space. (Note that this is not the same tensor product decomposition as the physical qubits; we are not even assuming there is a natural set of physical qubits here.) Also assume the errors map $\mathcal{H}_N$ to itself and that this is a QECC for set $\mathcal{E}$ of errors. Show that there exists unitary $U$ such that $U|_{|0\rangle \otimes B} = I$ (in which case $U$ can be the encoder) and $U^\dagger$ followed by discarding the $\mathcal{H}_A$ subspace acts as a decoder map for the QECC.

**Problem #2. Example stabilizer**

For each of the following sets of Paulis, determine if they define valid stabilizers. If so, give their parameters $[[n, k, d]]$.

a) Stabilizer is all products of these operators:

$$\begin{matrix} X & X & Z & Y & I \\ Z & Y & I & I & X \\ X & I & X & Z & Z \end{matrix}$$

b) Stabilizer is all products of these operators:

$$\begin{matrix} X & X & X & X & X & X \\ Y & Y & Y & Y & Y & Y \\ Z & Z & Z & Z & Z & Z \end{matrix}$$

c) In binary symplectic matrix form:

$$\left(\begin{array}{cccccc|cccccc} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

d) The stabilizer corresponding to the GF(4) linear code with the following parity check matrix:

$$\begin{pmatrix} 0 & 1 & 1 & \omega & \omega^2 \end{pmatrix}$$

**Problem #3. Stabilizer generating sets**

Suppose we have a set of stabilizer generators $\{M_1, \ldots, M_r\}$ for a stabilizer $S$ and $N \in S$ is not a generator. Show that we can remove an element of the original generating set and replace it with $N$ to get a new minimal generating set.

**Problem #4. Low-density parity check CSS codes**

A classical LDPC ("low density parity check") code is an $[n, k, d]$ linear code where each row of the parity check matrix has at most $r$ 1's and each column of the parity check matrix has at most $c$ 1's, with $r$ and $c$ of constant size (as $n$ gets large). (Sometimes LDPC codes with $r$ and $c$ increasing sublinearly with $n$ are also considered, but assume $r$ and $c$ are constant for the purposes of this problem.) Classical LDPC codes are interesting because they can achieve good values of $k/n$, $d/n$, and also generally have good decoding algorithms.

A quantum LDPC code is a stabilizer code for which each generator has low weight and each qubit appears in only a small number of generators. One might try to make good quantum LDPC codes using the CSS construction, based on pairs of classical LDPC codes $C_1(n)$ and $C_2(n)$. Suppose that one finds a family of such codes which produce $[[n, k, d]]$ quantum codes with $k/n$ and $d/n$ both constant as $n$ gets large. Show that this family of quantum codes must be degenerate for large $n$.

[No such family is known in the quantum case. The point of the problem is that, because degeneracy is important to find such codes, the quantum case is not a straightforward application of the CSS construction.]