Exercise Sheet 9

Quantum Information

To be returned no later than June 25, 2015

(20 points) **Problem 1: Quantum error-correction conditions.**

In this exercise we will rephrase a condition for the existence of an error-correcting code. Here the quantum code space is defined not by its basis, but by a projector onto it.

Let C be a quantum code, and let P be the projector onto C. Suppose $\mathcal{E}$ is a quantum operation with operation elements $\{E_j\}$. Prove that the following condition is necessary and sufficient for the existence of an error-correction operation $\mathcal{R}$ correcting $\mathcal{E}$ on C

$$PE_i^\dagger E_j P = \alpha_{ij} P,$$

for some Hermitian matrix α of complex numbers.

Hint: For necessity condition consider a state $P\rho P$ and note that it is in the code space for all ρ and therefore it has to be recoverable. Use the existence of the recovery operation $\mathcal{R} = \{R_j\}$ and write out this condition explicitly. You would see that two operations on ρ lead to the same result, and therefore these operations are unitarily equivalent. Write the equivalence condition. Using that $\mathcal{R}$ is trace-preserving operation deduce the necessary condition.

For sufficient condition, construct an explicit error-correction operation $\mathcal{R}$. Use the two-part form that was used for the Shor code - error-detection and then recovery. Diagonalize matrix α and let us denote $d = u^\dagger \alpha u$, where u is unitary and d is diagonal. Show that operators $F_k = \sum_i u_{ik} E_i$ are also a set of operation elements for $\mathcal{E}$. Show that $\{F_j\}$ satisfy a simpler (but similar) quantum error-correction condition than $\{E_j\}$. Use polar decomposition to find a projector onto a subspace onto with the coding subspace is rotated by F_k. These projectors (possibly with an additional projector) define a syndrome measurement. The recovery is performed by applying a transpose of a unitary that appeared in the polar decomposition previously. Write the corresponding quantum operation $\mathcal{R}$ and show that it indeed recovers any state ρ, i.e. show that $\mathcal{R}(\mathcal{E}(\rho)) \propto \rho$.

(20 points) **Problem 2: Verification of error-correction conditions.**

1) Consider the three qubit bit flip code with corresponding projector onto the code space $P = |000\rangle\langle 000| + |111\rangle\langle 111|$. The noise process this code protects against has operation elements

$$\{\sqrt{(1-p)^3}\, I, \sqrt{p(1-p)^2}\, X_1, \sqrt{p(1-p)^2}\, X_2, \sqrt{p(1-p)^2}\, X_3\},$$

where p is the probability that a bit flips. Note that this quantum operation is not trace-preserving, since we have omitted operation elements corresponding to bit flips on two and three qubits. Verify

the quantum error-correction conditions for this code and noise process.
2) Consider [[7,1,3]] Steane code code discussed in the lecture. Remind that this code can correct an error on any single qubit. Verify the quantum error-correction conditions for this code.

(20 points) **Problem 3: Quantum Hamming bound.**
Here we will prove quantum Hamming bound, therefore you may not use the bound a priori in this exercise. Remind that for a non-degenerate code there is measurement that can diagnose the error that occurred. In other words, a code with basis $\{|\bar{j}\rangle\}$ that satisfies a condition $\langle\bar{j}| E_a^\dagger E_b |\bar{i}\rangle = \delta_{ab}\delta_{ij}$ is non-degenerate. In this case each E_a take the code subspace to a set of mutually orthogonal "error subspaces."
A non-degenerate code encodes k qubits in n qubits in such a way that it can correct errors on any subset of t or fewer qubits.
- Suppose $j \leq t$ errors occurred. How many locations where these errors can occur?
- With each such set of location how many errors can occur?
- Combining previous calculations, what is the total number of error that may occur on t or fewer qubits?
- Assuming a non-degenerate code, each of the errors must correspond to an orthogonal how-big-dimensional space?
- All of these subspaces must be fitted into the total how-big dimensional space?
- Comparing the dimensions of these spaces will lead to the Hamming bound. Write it out providing explanations.

(20 points) **Problem 4: Classical codes.**
1) Let H be a parity check matrix such that any $d-1$ columns are linearly independent, but there exists a set of d linearly dependent columns. Show that the code defined by H has distance d.
2) *Singleton bound.* Show that an $[n, k, d]$ code must satisfy $n - k \geq d - 1$.
3) *Hamming code.* Suppose $r \geq 2$ is an integer and let H be the matrix whose columns are all $2r-1$ bit strings of length r which are not identically 0. This parity check matrix defines a linear code with $n = 2^r - 1$ and $k = 2^r - r - 1$, known as a Hamming code. Show that all Hamming codes have distance 3, and thus can correct an error on a single bit.
4) *Gilbert-Varshamov bound.* This bound is one of the bounds that are used to check whether or not codes with particular code parameters exist. Gilbert-Varshamov bound states that for large n there exist an $[n, k]$ error-correcting code protecting against error on t bits for some k such that

$$\frac{k}{n} \geq 1 - S\Big(\frac{2t}{n}\Big),$$

where $S(x) = -x \log x - (1-x)\log(1-x)$ is the binary Shannon entropy. Prove this bound.

(20 points) **Problem 5: [[7,1,3]] Steane code.**
Remind that in the construction of the Steane code $\mathrm{CSS}(C_1, C_2)$, code C_1 was taken to be [7,4,3] Hamming code and $C_2 = C_1^\perp$.

1) Verify that the parity check matrix of C_2 is equal to the transposed generator matrix of C_1.
2)Determine the codewords of C_2.