Problem Set 4  
CPSC 440/640 Quantum Algorithms  
Andreas Klappenecker

The assignment is due on Wednesday, November 8, before class.

**Problem 1.** Let $G_n$ denote the Pauli group $G_n = \{ \pm X(a)Z(b) | a, b \in \mathbb{F}_2^n \}$. Show that two matrices $A, B$ in $G_n$ either commute or anticommute, that is, $AB = \pm BA$.

**Problem 2.** Recall that the trace $\text{tr} P$ of a matrix $P$ is given by the sum of its diagonal elements, that is, $\text{tr} P = \sum P_{ii}$. It is easy to show that $\text{tr}(APA^{-1}) = \text{tr}(P)$ holds for all invertible matrices $A$.

Let $Q$ be a quantum code of length $n$. Let $P : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ denote the orthogonal projector onto $Q$, that is, $P$ is the unique linear map that satisfies $P^2 = P$, $P^\dagger = P$, and $\text{image}(P) = Q$. Prove that $\text{dim} Q = \text{tr} P$.

**Problem 3.** Recall that a group $G$ is a set with a binary operation $\circ : G \times G \to G$ such that (i) $a \circ (b \circ c) = (a \circ b) \circ c$ holds for all $a, b, c \in G$; (ii) there exists an element $1$ in $G$, called the identity, such that $a \circ 1 = 1 \circ a = a$ for all $a$ in $G$; (iii) for each $a$ in $G$ there exists an element $a^{-1}$ in $G$ such that $a \circ a^{-1} = a^{-1} \circ a = 1$. The group $G$ is called abelian if $a \circ b = b \circ a$ holds for all $a, b$ in $G$.

Let $S$ denote an abelian subgroup of the Pauli group $G_n$.

(a) Let $A$ be an element of $S$. Prove that the map $m_A : S \to S$ given by $m_A(x) = Ax$ is a bijective map (=one-to-one and onto).

(b) Prove that $P = |S|^{-1} \sum_{B \in S} B$ is an orthogonal projector.

(c) Prove that if the group $S$ has $2^{n-k}$ elements, then the quantum code given by the image of $P$ has dimension $2^k$.

**Problem 4.** Let $Q$ denote the quantum code $Q = \{ a|001\rangle + b|110\rangle | a, b \in \mathbb{C} \}$.

(a) Determine all matrices $A$ in $S$ such that $A|x\rangle = |x\rangle$ for all $|x\rangle$ in $Q$. Prove that this set forms an abelian group $T$.

(b) Let $P$ denote the orthogonal projector corresponding to the abelian group $T$, as define in the previous problem. Show that the image of $P$ is $Q$. 