Quantum Computing - Problem Set 3

Mateus de Oliveira Oliveira

School of Computer Science and Communication
KTH Royal Institute of Technology, 100-44, Stockholm, Sweden
mdeoliv@kth.se

1 Pauli Group and Stabilizers

Also recall that the Pauli group is defined as follows

$$G_1 = \{\pm I, \pm X, \pm Y, \pm Z, \pm iI, \pm iX, \pm iY, \pm iZ\} \qquad G_n = G_1^{\otimes n}$$

Also, a state $|\psi\rangle$ is stabilized by an element $g \in G^{\otimes n}$ if $g|\psi\rangle = |\psi\rangle$.

1. Show that if v_1 and v_2 are stabilized by a set $S \subseteq G^{\otimes n}$ then $\alpha v_1 + \beta v_2$ is also stabilized by S for complex numbers α, β. So a stabilizer set S defines a vector space V_S.
2. Show that $V_S = \cap_{g \in S} V_g$
3. Show that if V is a vector space stabilized by a set $S \subseteq G^{\otimes n}$ then S is a subgroup of $G^{\otimes n}$ where the operation is multiplication. Hint: what are the inverse elements of X, Y and Z?
4. Two elements g_1, g_2 commute if $g_1 g_2 = g_2 g_1$ and anticommute if $g_1 g_2 = -g_2 g_1$. Show that two elements $g_1, g_2 \in G_1$ either commute or anti-commute.
5. Generalize the item above by showing that two elements g_1, g_2 of G_n either commute or anticommute.
6. Let $g_1, g_2, ..., g_k$ be a set of generators for the group S. Show that S every element of S commutes if and only if $g_i g_j = g_j g_i$ for every $1 \leq i, j \leq k$.

2 The Five Qubit Flip Code

Recall that a $[n, k]$ quantum code C is nothing but a subpace of $(\mathbb{C}^2)^{\otimes n}$ of dimension 2^k. If S is a reduced set of generators of G_n then the code (i.e., the subspace) stabilized by S is denoted $C(S)$.

1. Show that the three qubit flip code spanned by the basis states $|000\rangle$ and $|111\rangle$ is stabilized by $\langle Z_1 Z_2, Z_2 Z_3\rangle$, where $\langle S\rangle$ is the group generated by S.
2. Show that the three qubit phase flip code spanned by $|+++\rangle$ and $|---\rangle$ is stabilized by $\langle X_1 x_2, X_2 X_3\rangle$
3. The five qubit code is the stabilizer code stabilized by $\langle g_1, g_2, g_3, g_4\rangle$ where
   - $g_1 = X_1 Z_2 Z_3 X_4 I_5$
   - $g_2 = I_1 X_2 Z_3 Z_4 X_5$
   - $g_3 = X_1 I_2 X_3 Z_4 Z_5$

– $g_4 = Z_1 X_2 I_3 X_4 Z_5$

Show that the five qubit code stabilizes the following 5 qubit states, which act as the logical 0 and logical 1:

$$|0_L\rangle = \frac{1}{4} \begin{array}{l}[|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle + |01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle \\ -|11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle - |10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle]\end{array}$$

$$|1_L\rangle = \frac{1}{4} \begin{array}{l}[|11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle + |10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle \\ -|00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle - |01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle]\end{array}$$

4. Show that the logical X and Z for the 5-qubit code are respectively $\overline{Z} = Z_1 Z_2 Z_3 Z_4 Z_5$ and $\overline{X} = X_1 X_2 X_3 X_4 X_5$

3 Correctable Sets of Errors

Recall that the centralizer of $S \subseteq G_n$ is defined by the set of all elements $h \in G_n$ such that $hg = gh$ for every $g \in S$. Assume that $-I \notin S$. Let $E = \{E_1, ..., E_k\} \subseteq G_n$ be a set of errors. Then one can show that E is a correctable set of errors if $E_i^\dagger E_j \notin Z(S) - S$ for all $1 \leq i, j \leq k$.

1. Since we already know that pauli operators either commute or anticommute, given a set of errors $E = \{E_1, ..., E_k\}$, how can we test if E is correctable for $C(S)$?
2. Use your answer to the last question to show that the 3 qubit flip code corrects $\{I, X_1, X_2, X_3\}$ and the phase flip code corrects $\{I, Z_1, Z_2, Z_3\}$.
3. Show that the five qubit code corrects against arbitrary 1-qubit errors.

4 Steane Code

Let C_1 be a $[n, k_1]$ code and C_2 a $[n, k_2]$ code such that $C_2 \subseteq C_1$ and such that both $C_2^\perp$ and C_1 correct t errors. We saw that we can define a $[n, k_1 - k_2]$ quantum code $CSS(C_1, C_2)$ that can correct errors on t qubits. Consider the parity check matrix of the $[7, 4, 3]$ Hamming code C:

$$H = \begin{bmatrix} 0\,0\,0\,1\,1\,1\,1 \\ 0\,1\,1\,0\,0\,1\,1 \\ 1\,0\,1\,0\,1\,0\,1 \end{bmatrix}$$

1. Let $C_1 = C$ and $C_2 = C^\perp$
2. Argue that both C_1 and $C_2^\perp$ can correct 1 error. (Hint: What is the distance of $C_2^\perp$?)
3. Show that $C_2 \subseteq C_1$. In other words the Hamming code can be used to construct a $[7, 1, 1]$ quantum code, which is called the Steane code.