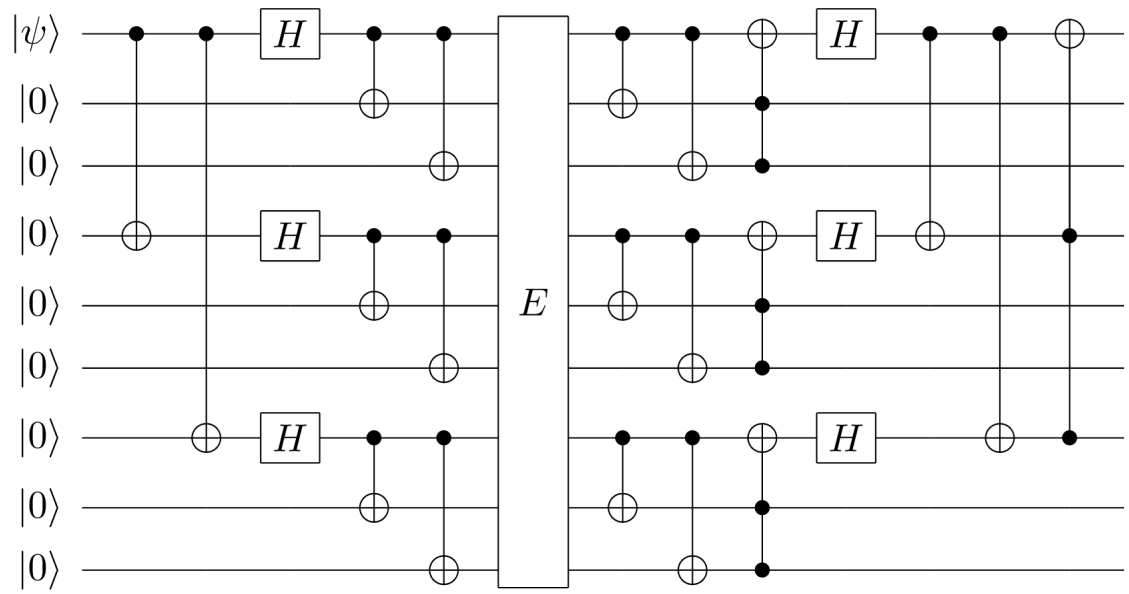
TUTORIAL 12

1 Assignment 9

1. Show that if a code $C \subset \{0,1\}^n$ corrects errors $E \subset \{0,1\}^n \times \{0,1\}^n$, then there exists a map $D : \{0,1\}^n \to C$ with the property:
$$\forall x \in C, (x,y) \in E \implies D(y) = x. \tag{1}$$
2. Let $C \subset \{0,1\}^n$ be a code of distance $d = 3$. Show that the blocklength n and the dimension k satisfy:
$$k \leq n - \log_2(n+1). \tag{2}$$

2 Computations around Shor's Code

We depict below Shor's code, followed by an error E and then followed by the decoding procedure:



1. Recall what is the encoded state before E.
2. Let us show that the decoding procedure works well for Pauli errors acting on the first register. Specifically, show that for the following E, we get back $|\psi\rangle$ in the first register:
   (a) $E = I^{\otimes 9}$
   (b) $E = X \otimes I^{\otimes 8}$
   (c) $E = Z \otimes I^{\otimes 8}$
   (d) $E = XZ \otimes I^{\otimes 8}$
3. Show that for any unitary U acting on 1 qubit, if $E = U \otimes I^{\otimes 8}$, then we get back $|\psi\rangle$ in the first register.
4. What can you say if E is acting on a single register, but not necessarily the first?

3 Stabilizer Codes

Definition 3.1. *Let S be a subgroup of the Pauli group $G_n := \{A_1 \otimes \ldots \otimes A_n, A_i \in G_1\}$, $G_1 := \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$. We define the stabilizer code $\mathcal{C}_S$ to be the vector subspace of $(\mathbb{C}^2)^{\otimes n}$ stabilized by S, i.e.:*

$$|\psi\rangle \in \mathcal{C}_S \Leftrightarrow \forall h \in S, h \cdot |\psi\rangle = |\psi\rangle \ .$$

1. First, let us consider the example where $n = 3$ and $S = \{I, Z_1Z_2, Z_1Z_3, Z_2Z_3\}$, with $Z_i := Z[i]$. Give a basis of $\mathcal{C}_S$.

2. Recall that a group G is generated by H if $G = \{h_1h_2 \ldots h_k : k \in \mathbb{N} \text{ and } \forall i \in [k], h_i \in H\}$, which we will denote by $G = \langle H \rangle$. Show that if S is a subgroup of G_n generated by H:

$$|\psi\rangle \in \mathcal{C}_S \Leftrightarrow \forall h \in H, h \cdot |\psi\rangle = |\psi\rangle \ .$$

   Thus, one can define a stabilizer code $\mathcal{C}_S$ only by considering a set of generators $\{g_1, \ldots, g_\ell\}$ of the group S.

3. Show that if $-I \in S$, then $\mathcal{C}_S = \{0\}$.

4. Show that if there exists a non-commuting pair of elements in $\{g_1, \ldots, g_\ell\}$, then $\mathcal{C}_{\langle g_1, \ldots, g_\ell \rangle} = \{0\}$.

   Remark. In fact, these necessary conditions of nontriviality are also sufficient: if $S = \langle g_1, \ldots, g_{n-k} \rangle$ with $n - k$ independent[1] commuting elements from G_n such that $-I \notin S$, then $\mathcal{C}_S$ is a subspace of dimension 2^k. □

5. Recall that the Shor code is defined by $|\overline{0}\rangle := \frac{1}{2\sqrt{2}} (|000\rangle + |111\rangle)^{\otimes 3}$ and $|\overline{1}\rangle := \frac{1}{2\sqrt{2}} (|000\rangle - |111\rangle)^{\otimes 3}$. Show that the Shor code is a stabilizer code, i.e. there exists $g_1, \ldots g_\ell$ such that $\mathcal{C}_{\langle g_1, \ldots g_\ell \rangle} = \text{span}\{|\overline{0}\rangle, |\overline{1}\rangle\}$ (you can use the previous remark without proving it).

[1] $\forall i \in [n-k], g_i \notin \langle g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_{n-k} \rangle$.