QMS Journal Club

Choong Pak Shen

January 15, 2026

QIntern x QMS Journal Club: Stabilizer formalism and introduction to quantum error correction

Outline

1. Introduction to classical error correction
2. Introduction to group theory
3. Introduction to stabilizer formalism
4. Introduction to cluster states

Introduction to classical error correction

In classical error correction, we encode message of k bits, $\vec{m}$ into n bits of codeword, $\vec{c}$, where $n-k$ bits are parity check bits, $\vec{p}$,

$$\vec{c} = \begin{pmatrix} c_1 \\ \vdots \\ c_k \\ c_{k+1} \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} \vec{m} \\ \vec{p} \end{pmatrix} \tag{1}$$

The parity check bits are set in such a way that the codeword $\vec{c}$ obeys $n-k$ linearly independent constraints, called parity checks $H(i)$,

$$H(i) \cdot \vec{c} = \sum_{j=1}^{n} H_j(i) c_j = 0, \tag{2}$$

where $i = 1, \ldots, n-k$.

Collecting the parity check vectors $H(i)$ into an $(n-k) \times n$ matrix,

$$H = \begin{pmatrix} - & H^T(1) & - \\ & \vdots & \\ - & H^T(n-k) & - \end{pmatrix}, \tag{3}$$

the set of parity checks can be written as a matrix equation $H\vec{c} = 0$.

A linear code $\mathcal{C}$ with $(n-k) \times n$ parity check matrix H consists of 2^k codewords $\vec{c} \in \mathbb{Z}_2^n$ that satisfies the set of parity checks $H\vec{c} = 0$.

The 2^k codewords form a k-dimensional vector subspace of $\mathbb{Z}_2^n$. $\mathcal{C}$ is referred to as an $[n, k]$ code.

The k-dimensional subspace is spanned by a set of k linearly independent bases,

$$\vec{c} = \sum_{j=1}^{k} m_j b_j \tag{4}$$

We can introduce an $(n \times k)$ matrix G, known as the generator matrix, such that

$$G = \begin{pmatrix} | & & | \\ b_1 & \dots & b_k \\ | & & | \end{pmatrix}. \tag{5}$$

Then, $\vec{c} = G\vec{m}$ and $HG\vec{m} = 0$. Notice that

$$HG = \begin{pmatrix} - & H^T(1) & - \\ & \vdots & \\ - & H^T(n-k) & - \end{pmatrix} \begin{pmatrix} | & & | \\ b_1 & \dots & b_k \\ | & & | \end{pmatrix} = 0. \tag{6}$$

The column space of H^T is orthogonal to the column space of G. Therefore, the column space of H^T is an $(n-k)$-dimensional vector space $\mathcal{C}^\perp \subset \mathbb{Z}_2^n$ and it is known as the dual code of $\mathcal{C}$.

Question: Let $\mathcal{C}$ be a $[6,3]$ code with the following parity check matrix H,

$$H = \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right). \tag{7}$$

Find the generator matrix G and the codewords of $\mathcal{C}$.

The Hamming distance $d(\vec{x}, \vec{y})$ between two vectors $\vec{x}$ and $\vec{y}$ is the number of places in which they differ, i.e. the number of positions i for which $x_i \neq y_i$.

It is a metric function in the sense that it satisfies the following three properties:

1. $d(\vec{x}, \vec{y}) = 0$ if and only if $\vec{x} = \vec{y}$;
2. $d(\vec{x}, \vec{y}) = d(\vec{y}, \vec{x})$;
3. $d(\vec{x}, \vec{y}) \leq d(\vec{x}, \vec{z}) + d(\vec{z}, \vec{y})$.

Question: Find the Hamming distance of $\vec{x} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ and $\vec{y} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$.

An important property of a code $\mathcal{C}$ is the minimum distance between codewords, denoted by d,

$$d = \min_{\vec{c},\vec{c}' \in \mathcal{C}} d(\vec{c}, \vec{c}'). \tag{8}$$

A linear code $\mathcal{C}$ with length n, dimension k, and minimum distance d will be referred to as an $[n, k, d]$ code. A linear code $\mathcal{C}$ witth minimum distance d can correct $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ bit errors.

The parity check matrix H for a code $\mathcal{C}$ produces a linear transformation from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^{n-k}$,

$$\vec{s} = H\vec{y}, \tag{9}$$

where $\vec{y} \in \mathbb{Z}_2^n$ and $\vec{s} \in \mathbb{Z}_2^{n-k}$ is the error syndrome.

If $\vec{y} \in \mathcal{C}$, then the parity check matrix H annihilates it ($H\vec{y} = 0$).

Example: Consider the code $\mathcal{C}$ with the parity check matrix

$$H = \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right). \tag{10}$$

The eight codewords are:

$$000000, 100110, 111000, 010101, 001011, 110011, 101101, 011110.$$

The minimum distance of the code $d = 3$, hence this is a $[6, 3, 3]$ code and can correct 1 error.

The standard array for this code is

000000	100110	111000	010101	001011	110011	101101	011110
000001	100111	111001	010100	001010	110010	101100	011111
000010	100100	111010	010111	001001	110001	101111	011100
000100	100010	111100	010001	001111	110111	101001	011010
001000	101110	110000	011101	000011	111011	100101	010110
010000	110110	101000	000101	011011	100011	111101	001110
100000	000110	011000	110101	101011	010011	001101	111110
100001	000111	011001	110100	101010	010010	001100	111111

Question: Study the following error detection and error correction:

1. $\vec{c} = 110011$ and $\vec{y} = 110001$
2. $\vec{c} = 110011$ and $\vec{y} = 111111$

Question: Construct the repetition code $[3, 1, 3]$ by finding the generator matrix G and parity check matrix H. Find the codewords $\vec{c}$.

Introduction to group theory

A group $(G, *)$ is a set G, together with a binary operation $*$ on G, such that the following axioms are satisfied:

1. The binary operation $*$ is associative, i.e. for $a, b, c \in G$, $a * (b * c) = (a * b) * c$.
2. There is an element e in G such that $e * a = a * e = a$ for all $a \in G$. This element e is an identity element for $*$ on G.
3. For each a in G, there is an element a' in G with the property that $a' * a = a * a' = e$. The element a' is an inverse of a with respect to $*$.
4. G is closed under the operation $*$, i.e. $a * b \in G$ for all $a, b \in G$.

Question: Are the following a group? Provide a reason if it is not a group.

1. The set of all positive integers, $\mathbb{Z}^+$ with operation $+$
2. The set of all positive integers, $\mathbb{Z}^+$ with operation $\times$
3. The set of all non-negative integers, $\mathbb{Z}^+ \cup \{0\}$ with operation $+$
4. The set of all integers, $\mathbb{Z}$ with operation $+$
5. The set of all positive rational numbers, $\mathbb{Q}^+$ with operation $\times$

For groups with finite set of elements (also called finite groups), one can construct the group multiplication table.

Consider a group with two elements, $\{e, a\}$ with binary operation $*$. The group multiplication table can be given by

$$Z_2 = \begin{array}{c|c|c} * & e & a \\ \hline e & e & a \\ \hline a & a & e \end{array}$$

Question: Consider a group with three elements, $\{e, a, b\}$ with binary operation $*$. Fill in the following group multiplication table.

$$Z_3 = \begin{array}{c|c|c|c} * & e & a & b \\ \hline e & e & a & b \\ \hline a & a & & \\ \hline b & b & & \end{array}$$

From the example of a finite group for three elements, it is obvious to see that in order to preserve the uniqueness of inverse elements and identity in G, each element of the group must appear once and only once in each row and column of the group multiplication table.

Since there is only one way to write the group multiplication tables for the finite group of two (three) elements, the structural features for all finite groups of two (three) elements are the same. In a less rigorous explanation, this is called group isomorphism.

Question: There are two group structures for finite group of four elements. Write down their group multiplication tables.

$Z_4 =$

$*$	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

$V =$

$*$	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

If H is a subset of a group G such that the group operation of G is closed on H, and if H is itself a group under the induced group operation on H from G, then H is a subgroup of G.

G and $\{e\}$ are improper subgroups of G. All other subgroups are proper subgroups.

Question: Identify if the following statements are true or false.

1. $(\mathbb{Z}, +)$ is a proper subgroup of $(\mathbb{R}, +)$.
2. $(\mathbb{Q}^+, \times)$ is a proper subgroup of $(\mathbb{R}, +)$.
3. $(\mathbb{Q}^+, \times)$ is a proper subgroup of $(\mathbb{R}^+, \times)$.

Question: Write down all the proper subgroups of Z_4 and V.

From the exercises, it is evident that H is a subgroup of G if and only if

1. the binary operation of G is closed on H
2. the identity e of G is in H
3. for all $a \in H$, it is true that its inverse $a' \in H$

Question: Using Z_4 and V as examples, how big a subgroup H of Z_4 and V needs respectively to be to contain the element $\{c\}$?

$$Z_4 = \begin{array}{|c|c|c|c|c|} \hline * & e & a & b & c \\ \hline e & e & a & b & c \\ \hline a & a & b & c & e \\ \hline b & b & c & e & a \\ \hline c & c & e & a & b \\ \hline \end{array} \qquad V = \begin{array}{|c|c|c|c|c|} \hline * & e & a & b & c \\ \hline e & e & a & b & c \\ \hline a & a & e & c & b \\ \hline b & b & c & e & a \\ \hline c & c & b & a & e \\ \hline \end{array}$$

Let G be a group and let $a \in G$. Then

$$H = \langle a \rangle = \{a^n | n \in \mathbb{Z}\} \tag{11}$$

is called a cyclic subgroup of G generated by a and is the smallest subgroup of G which contains a.

An element a of a group G generates G and is a generator for G is $\langle a \rangle = G$. A group G is cyclic if there is some element a in G which generates G.

Z_4 is cyclic since $\langle 1 \rangle = \langle 3 \rangle = Z_4$. V is not cyclic.

Question: Is $(\mathbb{Z}, +)$ cyclic?

Introduction to stabilizer formalism

The Pauli matrices are given by

$$\sigma_0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{12}$$

$$\sigma_1 = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{13}$$

$$\sigma_2 = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \tag{14}$$

$$\sigma_3 = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{15}$$

It is important to take note that

$$XY = iZ; YX = -iZ, \tag{16}$$

$$YZ = iX; ZY = -iX, \tag{17}$$

$$ZX = iY; XZ = -iY, \tag{18}$$

$$XX = YY = ZZ = I. \tag{19}$$

They form a Pauli group (of one qubit),

$$P_1 = \langle X, Y, Z \rangle = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}, \tag{20}$$

where $\{X, Y, Z\}$ are the generating set (generators) of the Pauli group.

In general, the Pauli group of n qubits is defined as

$$\begin{aligned} P_n &= \langle \sigma_{j_1} \otimes \ldots \otimes \sigma_{j_k} \otimes \ldots \otimes \sigma_{j_n} \rangle \\ &= \{ e^{\frac{i\theta\pi}{2}} \sigma_{j_1} \otimes \ldots \otimes \sigma_{j_k} \otimes \ldots \otimes \sigma_{j_n} \}, \end{aligned} \tag{21}$$

where $\theta = \{0, 1, 2, 3\}$ and $j_k = \{0, 1, 2, 3\}$.

When writing the elements in a Pauli group of n qubits, we usually omit the tensor product $\otimes$. For example, $X_1 Y_2 Z_3$ denotes $X \otimes Y \otimes Z$, a three-qubit Pauli group element where Pauli X acts on the first qubit, Pauli Y acts on the second qubit, and Pauli Z acts on the third qubit.

Pauli group of n qubits P_n acts on n-qubit state to produce another n-qubit state.

Suppose S is a subgroup of P_n and V_S is the set of n-qubit states which are fixed by every element of S. V_S is the vector space stabilized by S, and S is the stabilizer of the space V_S.

Recall that the Pauli matrices have two eigenvalues ± 1,

$$X|+\rangle = |+\rangle; X|-\rangle = -|-\rangle, \tag{22}$$

$$Y|+i\rangle = |+i\rangle; Y|-i\rangle = -|-i\rangle, \tag{23}$$

$$Z|0\rangle = |0\rangle; Z|1\rangle = -|1\rangle. \tag{24}$$

Question: Write down the subgroup $S = \langle X \rangle$. Find the set V_S that the subgroup S stabilizes.

Question: Write down the subgroup $S = \langle \pm X \rangle$. Find the set V_S that the subgroup S stabilizes.

Question: Find the set V_S that the Pauli group P_1 stabilizes.

Question: Write down the subgroup $S = \langle Z_1 Z_2, Z_2 Z_3 \rangle$. Find the set V_S that the subgroup S stabilizes.

From the given examples, we can conclude that

1. To check that a particular vector is stabilized by a subgroup S, we only need to check that the vector is stabilized by the generators;
2. In order for a subgroup S to stabilize a non-trivial vector space, the elements of S must commute, and $-I$ is not an element of S.

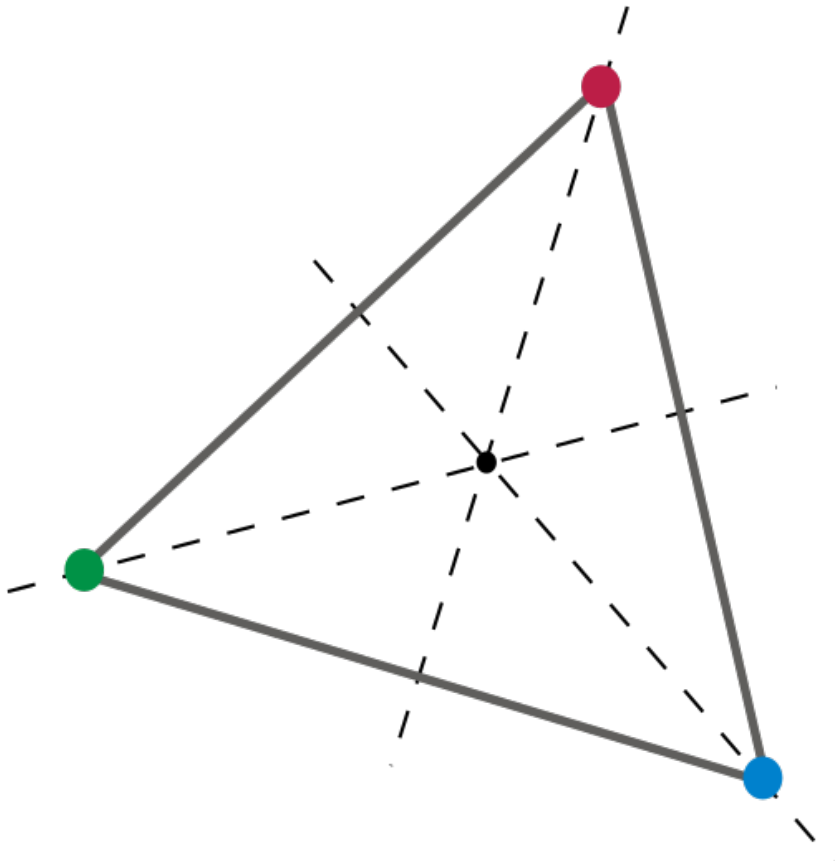
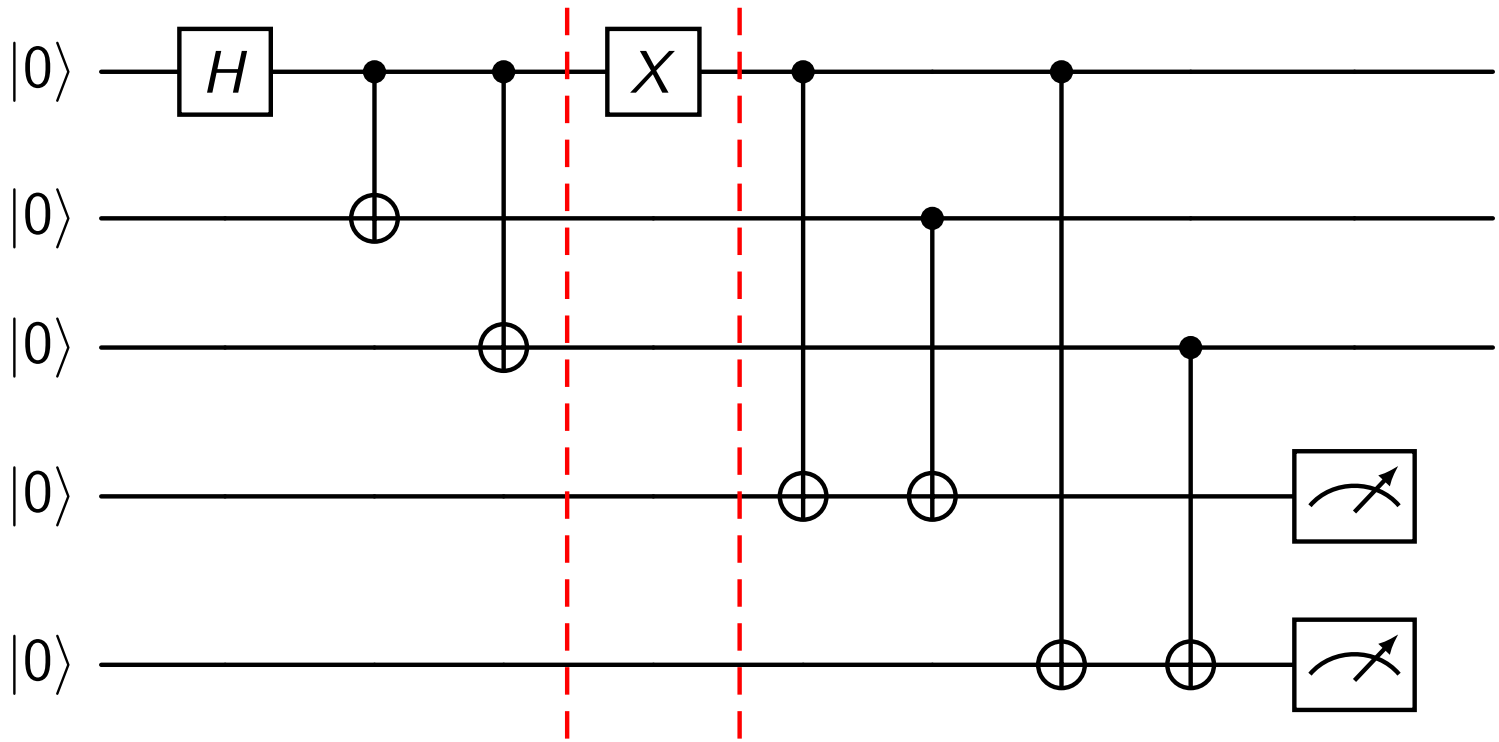


Figure 1: The cyclic group Z_3 consisting of the rotations by $0\pi, \frac{2\pi}{3}, \frac{4\pi}{3}$. The stabilizer group provides an alternative description to the vectors stabilized by the stabilizer group.

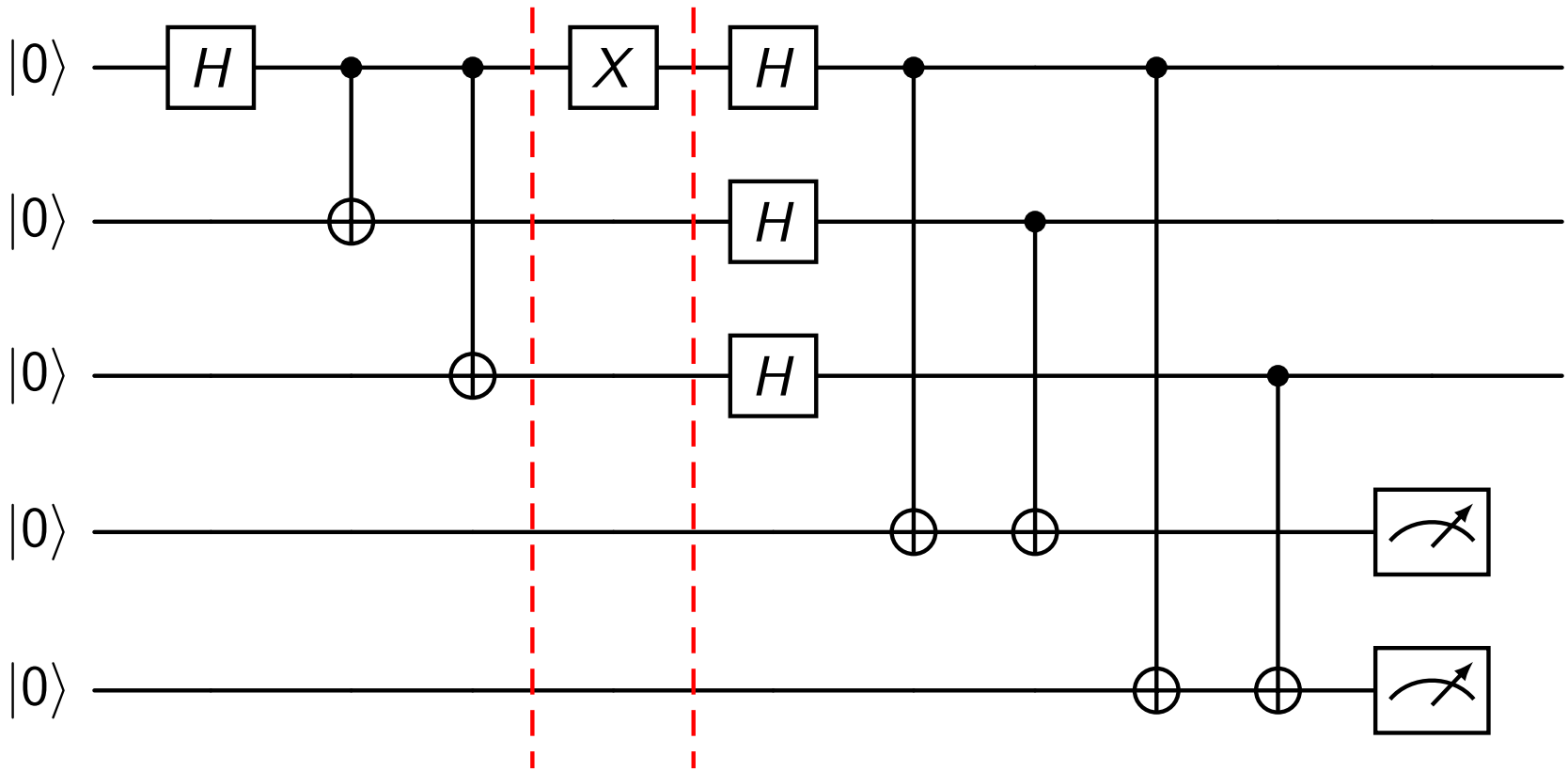
The three-qubit bit-flip code is given by



If a bit flip happened, we perform a parity measurement Z_1Z_2 and Z_2Z_3.

Error	Z_1Z_2I	Z_1IZ_3	IZ_2Z_3
III	$+1$	$+1$	$+1$
X_1II	-1	-1	$+1$
IX_2I	-1	$+1$	-1
IIX_3	$+1$	-1	-1

Question: The three-qubit phase-flip code is given as follow. What is the generating set of the stabilizers and the set V_S?

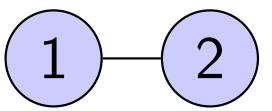


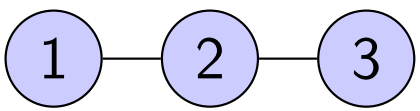
Introduction to cluster states

Cluster states are special graph states which are used in measurement-based quantum computing. The procedure to construct the cluster states is given as follow:

1. Begin with ground states $|0\rangle$ on all qubits;
2. Apply Hadamard gates on all qubits;
3. Apply control-Z gates on the qubits that are connected together.

Question: Write down the cluster states (pure states) for the following graphs.

1. 

2. 

The generating set of stabilizers for cluster states K can be given by

$$g_j = X_i \prod_{j \in N(i)} Z_j, \tag{25}$$

where $N(i)$ are the neighboring index.

Question: Find the generating set of the cluster states in the previous slide.

Question: By using the pure state form of the cluster states above, verify that the density matrices of the above cluster states are given by

$$\rho = \prod_{i=1}^{N} \frac{I_i + g_i}{2}. \tag{26}$$