\[ X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \]

We say that \( |\psi\rangle \) is stabilized by \( X_1 X_2 \) and by \( Z_1 Z_2 \). \( |\psi\rangle \) is the only state that up to a global phase is stabilized by \( X_1 X_2 \) and \( Z_1 Z_2 \). Quantum states with relevance for quantum error correction are often more compactly described by the stabilizer formalism.
\[ X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \]

\[ |\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \]
Stabilizer Codes

\[ X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \]

\[ |\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \]

\[ X_1 X_2 |\psi\rangle = |\psi\rangle \]

We say that \( |\psi\rangle \) is stabilized by \( X_1 X_2 \) and \( Z_1 Z_2 \).

\( |\psi\rangle \) is the only state that up to a global phase is stabilized by \( X_1 X_2 \) and \( Z_1 Z_2 \).

Quantum states with relevance for quantum error correction are often more compactly described by the stabilizer formalism.
Stabilizer Codes

- \( X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \)  
  \( Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \)

- \( |\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \)

- \( X_1 X_2 |\psi\rangle = |\psi\rangle \)

- \( Z_1 Z_2 |\psi\rangle = |\psi\rangle \)

We say that \( |\psi\rangle \) is stabilized by \( X_1 X_2 \) and by \( Z_1 Z_2 \).

|\psi\rangle is the only state that up to a global phase that is stabilized by \( X_1 X_2 \) and \( Z_1 Z_2 \).

Quantum states with relevance for quantum error correction are often more compactly described by the stabilizer formalism.
\[ X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \]

\[ |\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \]

\[ X_1 X_2 |\psi\rangle = |\psi\rangle \]

\[ Z_1 Z_2 |\psi\rangle = |\psi\rangle \]

We say that \( |\psi\rangle \) is stabilized by \( X_1 X_2 \) and by \( Z_1 Z_2 \).
Stabilizer Codes

\[ X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \]

\[ |\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \]

\[ X_1 X_2 |\psi\rangle = |\psi\rangle \]

\[ Z_1 Z_2 |\psi\rangle = |\psi\rangle \]

We say that \(|\psi\rangle\) is stabilized by \(X_1 X_2\) and by \(Z_1 Z_2\).

\(|\psi\rangle\) is the only state that up to a global phase that is stabilized by \(X_1 X_2\) and \(Z_1 Z_2\).
Stabilizer Codes

\[ X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \]

\[ |\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \]

\[ X_1 X_2 |\psi\rangle = |\psi\rangle \]
\[ Z_1 Z_2 |\psi\rangle = |\psi\rangle \]

We say that \(|\psi\rangle\) is stabilized by \(X_1 X_2\) and by \(Z_1 Z_2\).

\(|\psi\rangle\) is the only state that up to a global phase that is stabilized by \(X_1 X_2\) and \(Z_1 Z_2\).

Quantum states with relevance for quantum error correction are often more compactly described by the stabilizer formalism.
Stabilizer Codes

Pauli Matrices:

\[
I = \begin{bmatrix}
1 & 0 \\
0 & 1 \\
\end{bmatrix} \quad X = \begin{bmatrix}
0 & 1 \\
1 & 0 \\
\end{bmatrix} \quad Y = \begin{bmatrix}
0 & -i \\
i & 0 \\
\end{bmatrix} \quad Z = \begin{bmatrix}
1 & 0 \\
0 & -1 \\
\end{bmatrix}
\]
Pauli Matrices:

\[ I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \]

Pauli Group:

\[ G_1 = \{ \pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ \} \]
Pauli Matrices:

\[ I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \]

Pauli Group:

\[ G_1 = \{ \pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ \} \]

\( G_1 \) forms a group under matrix multiplication.
Pauli Matrices:

\[
I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}
\]

Pauli Group:

\[G_1 = \{ \pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ \}\]

\(G_1\) forms a group under matrix multiplication.

\(G_n = \{ P_1 \otimes P_2 \otimes ... \otimes P_n | P_i \in G_1 \}\)
Pauli Matrices:

\[ I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \]

Pauli Group:

\[ G_1 = \{ \pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ \} \]

\( G_1 \) forms a group under matrix multiplication.

\[ G_n = \{ P_1 \otimes P_2 \otimes \ldots \otimes P_n \mid P_i \in G_1 \} \]

\( G_n \) also forms a group under matrix multiplication.
Let $S$ be a subgroup of $G_n$.
- Let $S$ be a subgroup of $G_n$
- Define $V_S = \{ |\psi\rangle \in (\mathbb{C}^2)^\otimes n | M |\psi\rangle = |\psi\rangle \forall M \in G_n \}$
Let $S$ be a subgroup of $G_n$

Define $V_S = \{ |\psi\rangle \in (\mathbb{C}^2)^\otimes n | M |\psi\rangle = |\psi\rangle \forall M \in G_n \}$

In other words, $V_S$ is the set of $n$-qubit states that are stabilized by all matrices in $S$. 
Let $S$ be a subgroup of $G_n$

Define $V_S = \{ |\psi\rangle \in (\mathbb{C}^2)^\otimes n | M |\psi\rangle = |\psi\rangle \forall M \in G_n \}$

In other words, $V_S$ is the set of $n$-qubit states that are stabilized by all matrices in $S$.

Exercise: $V_S$ is a subspace of $(\mathbb{C}^2)^\otimes n$
Let $S$ be a subgroup of $G_n$

Define $V_S = \{ |\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \mid M|\psi\rangle = |\psi\rangle \forall M \in G_n \}$

In other words $V_S$ is the set of $n$-qubit states that are stabilized by all matrices in $S$.

Exercise: $V_S$ is a subspace of $(\mathbb{C}^2)^{\otimes n}$

$V_S$ is the intersection of all $V_x$ for $x \in S$
Example:
Example:

\[ S = \{ I, Z_1 Z_2, Z_1 Z_3, Z_2 Z_3 \} \]
Example:

\[ S = \{ I, Z_1 Z_2, Z_1 Z_3, Z_2 Z_3 \} \]
Example:

\[ S = \{ I, Z_1Z_2, Z_1Z_3, Z_2Z_3 \} \]

- \( Z_1Z_2: |000\rangle, |001\rangle, |110\rangle, |111\rangle \)
Example:

\[ S = \{ I, Z_1Z_2, Z_1Z_3, Z_2Z_3 \} \]

- \[ Z_1Z_2: |000\rangle, |001\rangle, |110\rangle, |111\rangle \]
- \[ Z_1Z_3: |000\rangle, |010\rangle, |101\rangle, |111\rangle \]

Then \[ V_S = \{ |000\rangle, |111\rangle \} \]

Obs: Any group can be generated by \[ \log |G| \]
Example:

\[ S = \{ I, Z_1 Z_2, Z_1 Z_3, Z_2 Z_3 \} \]

- \( Z_1 Z_2 \): \(|000\rangle, |001\rangle, |110\rangle, |111\rangle\)
- \( Z_1 Z_3 \): \(|000\rangle, |010\rangle, |101\rangle, |111\rangle\)
- \( Z_2 Z_3 \): \(|000\rangle, |100\rangle, |011\rangle, |111\rangle\)
Example:

\[ S = \{ I, Z_1Z_2, Z_1Z_3, Z_2Z_3 \} \]

- \( Z_1Z_2 \): \( |000\rangle, |001\rangle, |110\rangle, |111\rangle \)
- \( Z_1Z_3 \): \( |000\rangle, |010\rangle, |101\rangle, |111\rangle \)
- \( Z_2Z_3 \): \( |000\rangle, |100\rangle, |011\rangle, |111\rangle \)

Then \( V_S = \{ |000\rangle, |111\rangle \} \)
Example:

\[ S = \{ I, Z_1 Z_2, Z_1 Z_3, Z_2 Z_3 \} \]

- \( Z_1 Z_2 \):
  - \( |000\rangle, |001\rangle, |110\rangle, |111\rangle \)

- \( Z_1 Z_3 \):
  - \( |000\rangle, |010\rangle, |101\rangle, |111\rangle \)

- \( Z_2 Z_3 \):
  - \( |000\rangle, |100\rangle, |011\rangle, |111\rangle \)

Then \( V_S = \{ |000\rangle, |111\rangle \} \)

Obs: Any group can be generated by \( \log |G| \)
Let $S$ be a subset of the Pauli group. $V_S$ is non trivial iff

- The elements of $S$ commute.

- Suppose elements $M, N$ anticommute: $MN = -NM$.

Then $|\psi\rangle = MN|\psi\rangle = -NM|\psi\rangle = |\psi\rangle$.

$-I$ is not an element of $S$.

If $-I \in S$ then $-I|\psi\rangle = |\psi\rangle$ then $|\psi\rangle = 0$.

Easy exercise: If $S$ is a subgroup of $G_n$ generated by elements $g_1, \ldots, g_l$ then all elements of $S$ commute iff $g_i g_j$ commute for every $i, j$. 
Let $S$ be a subset of the Pauli group. $V_S$ is non trivial iff

- The elements of $S$ commute
  - The elements of the Pauli Group either commute or anticommute.
  - Suppose elements $M, N$ anticommute: $MN = -NM$
  - Then $|\psi\rangle = MN|\psi\rangle = -NM|\psi\rangle = |\psi\rangle$

- $-I$ is not an element of $S$
- If $-I \in S$ then $-I|\psi\rangle = |\psi\rangle$ then $|\psi\rangle = 0$.

Easy exercise: If $S$ is a subgroup of $G_n$ generated by elements $g_1, \ldots, g_l$ then all elements of $S$ commute iff $g_i g_j$ commute for every $i, j$. 
Let $S$ be a subset of the Pauli group. $V_S$ is non trivial iff

- The elements of $S$ commute
  - The elements of the Pauli Group either commute or anticommute.
  - Suppose elements $M, N$ anticommute: $MN = -NM$
  - Then $|\psi\rangle = MN|\psi\rangle = -NM|\psi\rangle = |\psi\rangle$
- $-I$ is not an element of $S$.
  - If $-I \in S$ then $-I|\psi\rangle = |\psi\rangle$ then $|\psi\rangle = 0$. 

Easy exercise: If $S$ is a subgroup of $G_n$ generated by elements $g_1, \ldots, g_l$ then all elements of $S$ commute iff $g_i g_j$ commute for every $i, j$. 

Mateus de Oliveira Oliveira (TCS-KTH)  Quantum Computation - Lecture 08 - Quantum Error Correction II
Let $S$ be a subset of the Pauli group. $V_S$ is non trivial iff

- The elements of $S$ commute
  - The elements of the Pauli Group either commute or anticommute.
  - Suppose elements $M, N$ anticommute: $MN = -NM$
  - Then $|\psi\rangle = MN|\psi\rangle = -NM|\psi\rangle = |\psi\rangle$
- $-I$ is not an element of $S$.
  - If $-I \in S$ then $-I|\psi\rangle = |\psi\rangle$ then $|\psi\rangle = 0$.

Easy exercise: If $S$ is a subgroup of $G_n$ generated by elements $g_1, \ldots, g_l$ then all elements of $S$ commute iff $g_i g_j$ commute for every $i, j$. 
Action of a unitary on a stabilized set.

Suppose $V_S$ is a subspace stabilized by a subgroup $S$ generated by $g_1, g_2, \ldots, g_r$.
Examples of Stabilizer Codes

Action of a unitary on a stabilized set.

- Suppose $V_S$ is a subspace stabilized by a subgroup $S$ generated by $g_1, g_2, \ldots, g_r$.
- We have that $U|\psi\rangle = Ug|\psi\rangle = Ugl|\psi\rangle = UgU^\dagger U|\psi\rangle$. 
Action of a unitary on a stabilized set.

- Suppose $V_S$ is a subspace stabilized by a subgroup $S$ generated by $g_1, g_2, \ldots, g_r$.
- We have that $U\ket{\psi} = Ug\ket{\psi} = Ugl\ket{\psi} = UgU^\dagger U\ket{\psi}$.
- Which means that $UgU^\dagger$ stabilizes $U\ket{\psi}$.
Action of a unitary on a stabilized set.

- Suppose $V_S$ is a subspace stabilized by a subgroup $S$ generated by $g_1, g_2, \ldots, g_r$.
- We have that $U|\psi\rangle = Ug|\psi\rangle = Ugl|\psi\rangle = UgU^\dagger U|\psi\rangle$.
- Which means that $UgU^\dagger$ stabilizes $U|\psi\rangle$.
- The vector space $V_S$ is stabilized by the group

$$\{UgU^\dagger | g \in S\}$$
Action of a unitary on a stabilized set.

- Suppose $V_S$ is a subspace stabilized by a subgroup $S$ generated by $g_1, g_2, \ldots, g_r$.
- We have that $U|\psi\rangle = Ug|\psi\rangle = Ugl|\psi\rangle = UgU^\dagger U|\psi\rangle$.
- Which means that $UgU^\dagger$ stabilizes $U|\psi\rangle$.
- The vector space $V_S$ is stabilized by the group 
\[ \{UgU^\dagger | g \in S\} \]

- More: If $g_1, g_2, \ldots, g_k$ generate $S$ then $Ug_1U^\dagger \ldots Ug_kU^\dagger$ generate $USU^\dagger$. 
Examples of Stabilizer Codes

- $H X H^\dagger = Z$

$|0\rangle$ is the only 1-qubit state stabilized by $Z$

$|+\rangle$ is the only 1-qubit state stabilized by $X$

We have that $H |0\rangle$ is stabilized by $H Z H^\dagger = |+\rangle \langle Z|^{n}$

$|0\rangle \otimes^n$ is stabilized by $\langle X|_1 \otimes \langle X|_2 \otimes \ldots \otimes \langle X|_n$.

Observe that we need $2^n$ amplitudes to specify this last state.
Examples of Stabilizer Codes

- $HXX^\dagger = Z$
- $HYH^\dagger = -Y$

$|0\rangle$ is the only 1-qubit state stabilized by $Z$.

$|+\rangle$ is the only 1-qubit state stabilized by $X$.

We have that $H|0\rangle$ is stabilized by $HZH^\dagger$.

$|0\rangle \otimes^n$ is stabilized by $\langle Z_{1}, Z_{2}, \ldots, Z_{n} \rangle$.

$|+\rangle \otimes^n$ is stabilized by $\langle X_{1}, X_{2}, \ldots, X_{n} \rangle$.

Observe that we need $2^n$ amplitudes to specify this last state.
Examples of Stabilizer Codes

- \( HXH^\dagger = Z \)
- \( HYH^\dagger = -Y \)
- \( HZH^\dagger = X \)

\( |0\rangle \) is the only 1-qubit state stabilized by \( Z \).
\( |+\rangle \) is the only 1-qubit state stabilized by \( X \).
We have that \( H |0\rangle \) is stabilized by \( HZH^\dagger \).
\( |0\rangle \otimes^n \langle X_{1}, X_{2}, \ldots, X_{n} | \) stabilizes \( |+\rangle \otimes^n \).
Observe that we need \( 2^n \) amplitudes to specify this last state.
Examples of Stabilizer Codes

- $HXH^\dagger = Z$
- $HYH^\dagger = -Y$
- $HZH^\dagger = X$
- $|0\rangle$ is the only 1-qubit state stabilized by $Z$

$|0\rangle$ stabilizes $\langle Z_1, Z_2, ..., Z_n |\langle X_1, X_2, ..., X_n |$ stabilizes $|+\rangle \otimes n$

Observe that we need $2^n$ amplitudes to specify this last state.
Examples of Stabilizer Codes

- $HXY^\dagger = Z$
- $HYH^\dagger = -Y$
- $HZH^\dagger = X$
- $|0\rangle$ is the only 1-qubit state stabilized by $Z$
- $|+\rangle$ is the only 1-qubit state stabilized by $X$
Examples of Stabilizer Codes

- \( HXH^\dagger = Z \)
- \( HYH^\dagger = -Y \)
- \( HZH^\dagger = X \)
- \( |0\rangle \) is the only 1-qubit state stabilized by \( Z \)
- \( |+\rangle \) is the only 1-qubit state stabilized by \( X \)
- We have that \( H|0\rangle \) is stabilized by \( HZH^\dagger = |+\rangle \)
Examples of Stabilizer Codes

- $HXH^\dagger = Z$
- $HYH^\dagger = -Y$
- $HZH^\dagger = X$
- $|0\rangle$ is the only 1-qubit state stabilized by $Z$
- $|+\rangle$ is the only 1-qubit state stabilized by $X$
- We have that $H|0\rangle$ is stabilized by $HZH^\dagger = |+\rangle$
- $\langle Z_1, Z_2, \ldots, Z_n \rangle$ stabilizes $|0\rangle \otimes^n$
Examples of Stabilizer Codes

- $H X H^\dagger = Z$
- $H Y H^\dagger = -Y$
- $H Z H^\dagger = X$
- $|0\rangle$ is the only 1-qubit state stabilized by $Z$
- $|+\rangle$ is the only 1-qubit state stabilized by $X$
- We have that $H |0\rangle$ is stabilized by $H Z H^\dagger = |+\rangle$
- $\langle Z_1, Z_2, \ldots, Z_n \rangle$ stabilizes $|0\rangle^{\otimes n}$
- $\langle X_1, X_2, \ldots, X_n \rangle$ stabilizes $|+\rangle^{\otimes n}$
Examples of Stabilizer Codes

- $H X H^\dagger = Z$
- $H Y H^\dagger = -Y$
- $H Z H^\dagger = X$
- $|0\rangle$ is the only 1-qubit state stabilized by $Z$
- $|+\rangle$ is the only 1-qubit state stabilized by $X$
- We have that $H |0\rangle$ is stabilized by $H Z H^\dagger = |+\rangle$
- $\langle Z_1, Z_2, \ldots, Z_n \rangle$ stabilizes $|0\rangle^\otimes n$
- $\langle X_1, X_2, \ldots, X_n \rangle$ stabilizes $|+\rangle^\otimes n$
- Observe that we need $2^n$ amplitudes to specify this last state
Let $U$ be the controlled-not.

- $UX_1 U^\dagger = X_1 X_2$
Let $U$ be the controlled-not.

- $UX_1 U^\dagger = X_1 X_2$
- $UX_2 U^\dagger = X_2$
Let $U$ be the controlled-not.

- $UX_1 U^\dagger = X_1 X_2$
- $UX_2 U^\dagger = X_2$
- $UZ_1 U^\dagger = Z_1$
Let $U$ be the controlled-not.

- $UX_1 U^\dagger = X_1 X_2$
- $UX_2 U^\dagger = X_2$
- $UZ_1 U^\dagger = Z_1$
- $UZ_2 U^\dagger = Z_1 Z_2$
Examples of Stabilizer Codes

Let \( S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \)

\[
SXS^\dagger = Y \quad SZS^\dagger = Z
\]

(1)

- Any unitary \( U \) that \( UG_n U^\dagger = G_n \) can be composed from Hadamard, phase and C-NOT gates.
Let $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$

\[ SXS^\dagger = Y \quad SZS^\dagger = Z \] (1)

- Any unitary $U$ that $UG_nU^\dagger = G_n$ can be composed from Hadamard, phase and C-NOT gates.
- The set of all unitaries $U$ such that $UgU^\dagger \in G_n$ for $g \in G_n$ is called the normalizer of $G_n$. 
Recalling:

- An observable is an Hermitian Operator on the state space of the system being observed.
Recalling:

- An observable is an Hermitian Operator on the state space of the system being observed.
- A projective Measurement is described by an observable $M$ whose spectral decomposition is

$$M = \sum_{m} mP_{m}$$
Recalling:

- An observable is an Hermitian Operator on the state space of the system being observed.
- A projective Measurement is described by an observable $M$ whose spectral decomposition is
  \[ M = \sum_{m} mP_m \]
  where $P_m$ is the projector onto the eigenspace of $M$ with eigenvalue $m$. 

The possible outcomes of the measurements correspond to the eigenvalues $m$ of the observable. The probability of getting the result $m$ is given by
  \[ p(m) = \langle \psi | P_m | \psi \rangle \] 
Given that the outcome $m$ occurred, the state of the quantum system immediately after the measurement is
  \[ P_m |\psi\rangle \sqrt{p(m)} \]
Recalling:

- An observable is an Hermitian Operator on the state space of the system being observed.
- A projective Measurement is described by an observable $M$ whose spectral decomposition is

$$M = \sum_m m P_m$$

- where $P_m$ is the projector onto the eigenspace of $M$ with eigenvalue $m$.
- The possible outcomes of the measurements correspond to the eigenvalues $m$ of the observable.
Recalling:

- An observable is an Hermitian Operator on the state space of the system being observed.
- A projective Measurement is described by an observable $M$ whose spectral decomposition is

$$M = \sum_m mP_m$$

where $P_m$ is the projector onto the eigenspace of $M$ with eigenvalue $m$.

- The possible outcomes of the measurements correspond to the eigenvalues $m$ of the observable.
- The probability of getting the result $m$ is given by $p(m) = \langle \psi | P | \psi \rangle$
Recalling:

- An observable is an Hermitian Operator on the state space of the system being observed.
- A projective Measurement is described by an observable $M$ whose spectral decomposition is

$$M = \sum_m m P_m$$

where $P_m$ is the projector onto the eigenspace of $M$ with eigenvalue $m$.
- The possible outcomes of the measurements correspond to the eigenvalues $m$ of the observable.
- The probability of getting the result $m$ is given by $p(m) = \langle \psi | P | \psi \rangle$
- Given that the outcome $m$ occurred, the state of the quantum system immediately after the measurement is

$$\frac{P_m | \psi \rangle}{\sqrt{p(m)}}$$
Let $g \in G_n$. 
Let $g \in G_n$. Since $g$ is a Hermitian operator, it can be regarded as an observable.
Let \( g \in G_n \).

Since \( g \) is a Hermitian operator, it can be regarded as an observable.

Assume the system is in state \( |\psi\rangle \) with stabilizer \( \langle g_1, \ldots, g_n \rangle \).
Let $g \in G_n$.

Since $g$ is a Hermitian operator, it can be regarded as an observable.

Assume the system is in state $|\psi\rangle$ with stabilizer $\langle g_1, \ldots, g_n \rangle$.

There are two possibilities for $g \in G_n$:

- $g$ commutes with all the generators of the stabilizer
- $g$ anti-commutes with one or more of the generators of the stabilizer.

In this case it anticommutes with a unique generator, say $g_1$, and commutes with all the others $g_2, \ldots, g_n$.

Suppose it anticommutes with $g_2$. Then it commutes with $g_1 g_2$. Then replace $g_2$ by $g_1 g_2$. 
Let $g \in G_n$.

Since $g$ is a Hermitian operator, it can be regarded as an observable.

Assume the system is in state $|\psi\rangle$ with stabilizer $\langle g_1, \ldots, g_n \rangle$.

There are two possibilities for $g \in G_n$:

- $g$ commutes with all the generators of the stabilizer.
- $g$ anti-commutes with one or more of the generators of the stabilizer.

In this case it anticommutes with a unique generator, say $g_1$ and commutes with all the others $g_2, \ldots, g_n$.

Suppose it anticommutes with $g_2$. Then it commutes with $g_1 g_2$. Then replace $g_2$ by $g_1 g_2$. 
• Let $g \in G_n$.
• Since $g$ is a Hermitian operator, it can be regarded as an observable.
• Assume the system is in state $|\psi\rangle$ with stabilizer $\langle g_1, \ldots, g_n \rangle$.
• There are two possibilities for $g \in G_n$:
  ▶ $g$ commutes with all the generators of the stabilizer
  ▶ $g$ anti-commutes with one or more of the generators of the stabilizer.
Let \( g \in G_n \).

Since \( g \) is a Hermitian operator, it can be regarded as an observable.

Assume the system is in state \( |\psi\rangle \) with stabilizer \( \langle g_1, \ldots, g_n \rangle \).

There are two possibilities for \( g \in G_n \):

- \( g \) commutes with all the generators of the stabilizer
- \( g \) anti-commutes with one or more of the generators of the stabilizer.

  - In this case it anticommutes with a unique generator, say \( g_1 \) and commutes with all the others \( g_2, \ldots, g_n \).
Let $g \in G_n$.

Since $g$ is a Hermitian operator, it can be regarded as an observable.

Assume the system is in state $|\psi\rangle$ with stabilizer $\langle g_1, \ldots, g_n \rangle$.

There are two possibilities for $g \in G_n$:

- $g$ commutes with all the generators of the stabilizer
- $g$ anti-commutes with one or more of the generators of the stabilizer.
  
  - In this case it anticommutes with a unique generator, say $g_1$ and commutes with all the others $g_2, \ldots, g_n$
  - Suppose it anticommutes with $g_2$. Then it commutes with $g_1 g_2$. Then replace $g_2$ by $g_1 g_2$.  

• $g$ commutes with all generators.

• $g$ anticommutes with some generator, say $g_1$. 
• $g$ commutes with all generators.
  ▶ Then either $g$ or $-g$ is an element of the stabilizer

• $g$ anticommutes with some generator, say $g_1$. 
- $g$ commutes with all generators.
  - Then either $g$ or $-g$ is an element of the stabilizer.
  - Since $g_j g |\psi\rangle = g g_j |\psi\rangle = g |\psi\rangle$ for each stabilizer generator, $g |\psi\rangle$ is in $V_S$ and thus a multiple of $|\psi\rangle$.

- $g$ anticommutes with some generator, say $g_1$. 

- $g$ commutes with all generators.
  - Then either $g$ or $-g$ is an element of the stabilizer
  - Since $g_j g |\psi\rangle = g g_j |\psi\rangle = g |\psi\rangle$ for each stabilizer generator, $g |\psi\rangle$ is in $V_S$ and thus a multiple of $|\psi\rangle$.
  - Since $g^2 = I$, it follows that $g |\psi\rangle = \pm |\psi\rangle$

- $g$ anticommutes with some generator, say $g_1$.
• $g$ commutes with all generators.
  ▶ Then either $g$ or $-g$ is an element of the stabilizer
  ▶ Since $g_j g |\psi\rangle = gg_j |\psi\rangle = g |\psi\rangle$ for each stabilizer generator, $g |\psi\rangle$ is in $V_S$ and thus a multiple of $|\psi\rangle$.
  ▶ Since $g^2 = I$, it follows that $g |\psi\rangle = \pm |\psi\rangle$
  ▶ Then either $g$ or $-g$ must be in the stabilizer.

• $g$ anticommutes with some generator, say $g_1$. 
• $g$ commutes with all generators.
  ▶ Then either $g$ or $-g$ is an element of the stabilizer.
  ▶ Since $g_j g |\psi\rangle = g g_j |\psi\rangle = g |\psi\rangle$ for each stabilizer generator, $g |\psi\rangle$ is in $V_S$ and thus a multiple of $|\psi\rangle$.
  ▶ Since $g^2 = I$, it follows that $g |\psi\rangle = \pm |\psi\rangle$.
  ▶ Then either $g$ or $-g$ must be in the stabilizer.
  ▶ Assume $g \in S$ the same holds for $-g \in S$. Then $g |\psi\rangle = |\psi\rangle$, and thus measuring $g$ gives the eigenvalue $+1$ with probability 1.

• $g$ anticommutes with some generator, say $g_1$. 
• $g$ commutes with all generators.
  ▶ Then either $g$ or $-g$ is an element of the stabilizer
  ▶ Since $g_j g |\psi\rangle = gg_j |\psi\rangle = g |\psi\rangle$ for each stabilizer generator, $g |\psi\rangle$ is in $V_S$ and thus a multiple of $|\psi\rangle$.
  ▶ Since $g^2 = I$, it follows that $g |\psi\rangle = \pm |\psi\rangle$
  ▶ Then either $g$ or $-g$ must be in the stabilizer.
  ▶ Assume $g \in S$ the same holds for $-g \in S$. Then $g |\psi\rangle = |\psi\rangle$, and thus measuring $g$ gives the eigenvalue $+1$ with probability 1.

• $g$ anticommutes with some generator, say $g_1$.
  ▶ $g$ has eigenvalue $\pm 1$
• $g$ commutes with all generators.
  ▶ Then either $g$ or $-g$ is an element of the stabilizer
  ▶ Since $g_j g |\psi\rangle = g g_j |\psi\rangle = g |\psi\rangle$ for each stabilizer generator, $g |\psi\rangle$ is in $V_S$ and thus a multiple of $|\psi\rangle$.
  ▶ Since $g^2 = I$, it follows that $g |\psi\rangle = \pm |\psi\rangle$
  ▶ Then either $g$ or $-g$ must be in the stabilizer.
  ▶ Assume $g \in S$ the same holds for $-g \in S$. Then $g |\psi\rangle = |\psi\rangle$, and thus measuring $g$ gives the eigenvalue $+1$ with probability $1$.

• $g$ anticommutes with some generator, say $g_1$.
  ▶ $g$ has eigenvalue $\pm 1$
  ▶ Thus the projectors for the measurement outcomes $\pm 1$ are given by $(I \pm g)/2$, respectively and thus the measurement probabilities are given by

\[
p(+1) = tr\left(\frac{1}{2}(I + g) |\psi\rangle \langle \psi| \right) \\
p(-1) = tr\left(\frac{1}{2}(I - g) |\psi\rangle \langle \psi| \right)
\]
One can see that $p(+1) = p(-1) = 1/2$
One can see that \( p(+1) = p(-1) = 1/2 \)

If the result +1 occurs, the result collapses to \( |\psi^+\rangle \equiv (I + g)|\psi\rangle/\sqrt{2} \), which has stabilizer \( \langle g_1, g_2, \ldots, g_n \rangle \).
One can see that $p(+1) = p(-1) = 1/2$

If the result $+1$ occurs, the result collapses to $|\psi^+\rangle \equiv (I + g)|\psi\rangle/\sqrt{2}$, which has stabilizer $\langle g_1, g_2, \ldots, g_n \rangle$.

If the result is $-1$ then the posterior state is stabilized to $\langle -g_1, g_2, \ldots, g_n \rangle$
The stabilizer formalism is well suited for the description of error correcting codes.
• The stabilizer formalism is well suited for the description of error correcting codes.

• \([n, k]\) stabilizer code: Vector space \(V_S\) stabilized by a subgroup \(S\) of \(G_n\) such that \(-I \notin S\) and \(S\) has \(n - k\) independent and commuting generators, \(S = \langle g_1, \ldots, g_{n-k} \rangle\).
The stabilizer formalism is well suited for the description of error correcting codes.

\([n, k]\) stabilizer code: Vector space \(V_S\) stabilized by a subgroup \(S\) of \(G_n\) such that \(-I \notin S\) and \(S\) has \(n - k\) independent and commuting generators, \(S = \langle g_1, \ldots, g_{n-k} \rangle\).

By independent generators we mean that removing any of the \(g_i\)'s makes the code shorter.
The stabilizer formalism is well suited for the description of error correcting codes.

$[n, k]$ stabilizer code: Vector space $V_S$ stabilized by a subgroup $S$ of $G_n$ such that $-I \notin S$ and $S$ has $n - k$ independent and commuting generators, $S = \langle g_1, ..., g_{n-k} \rangle$.

By independent generators we mean that removing any of the $g_i$'s makes the code shorter.

Denote this code by $C(S)$.
Encoding Qubits:

- Chose operators $\overline{Z}_1, \ldots, \overline{Z}_k$ such that $g_1, \ldots, g_{n-k}$, $\overline{Z}_1, \ldots, \overline{Z}_k$ forms and independent and commuting set.
Encoding Qubits:

- Chose operators $\overline{Z}_1, \ldots, \overline{Z}_k$ such that $g_1, \ldots, g_{n-k}, \overline{Z}_1, \ldots, \overline{Z}_k$ forms and independent and commuting set.
- $\overline{Z}_i$ play the role of a logical pauli $Z$ operator on qubit $i$. 
Encoding Qubits:

- Chose operators $\overline{Z}_1, ..., \overline{Z}_k$ such that $g_1, ..., g_{n-k}, \overline{Z}_1, ..., \overline{Z}_k$ forms and independent and commuting set.
- $\overline{Z}_i$ play the role of a logical pauli $Z$ operator on qubit $i$.
- The logical basis state $|x_1, ..., x_k\rangle_L$ is defined to be the state with stabilizer

$$\langle g_1, ..., g_{n-k}, (-1)^{x_1}\overline{Z}_1, ..., (-1)^{x_k}\overline{Z}_k \rangle$$
Encoding Qubits:

- Choose operators $\overline{Z}_1, \ldots, \overline{Z}_k$ such that $g_1, \ldots, g_{n-k}, \overline{Z}_1, \ldots, \overline{Z}_k$ forms and independent and commuting set.
- $\overline{Z}_i$ play the role of a logical pauli $Z$ operator on qubit $i$
- The logical basis state $|x_1, \ldots, x_k\rangle_L$ is defined to be the state with stabilizer
  \[
  \langle g_1, \ldots, g_{n-k}, (-1)^{x_1} \overline{Z}_1, \ldots, (-1)^{x_k} \overline{Z}_k \rangle
  \]
- Choose operators $\overline{X}_j$ which sends $\overline{Z}_j$ to $-\overline{Z}_j$ and leaves all other $Z_i$ and $g_i$ alone under conjugation.
Encoding Qubits:

- Chose operators $\overline{Z}_1, \ldots, \overline{Z}_k$ such that $g_1, \ldots, g_{n-k}, \overline{Z}_1, \ldots, \overline{Z}_k$ forms and independent and commuting set.
- $\overline{Z}_i$ play the role of a logical pauli $Z$ operator on qubit $i$.
- The logical basis state $|x_1, \ldots, x_k\rangle_L$ is defined to be the state with stabilizer
  $$\langle g_1, \ldots, g_{n-k}, (-1)^{x_1}\overline{Z}_1, \ldots, (-1)^{x_k}\overline{Z}_k\rangle$$
- Choose operators $\overline{X}_j$ which sends $\overline{Z}_j$ to $-\overline{Z}_j$ and leaves all other $Z_i$ and $g_i$ alone under conjugation.
- $\overline{X}_j$ has the effect of a quantum NOT gate acting on the $j$-th encoded qubit.
Encoding Qubits:

- Choose operators $\overline{Z}_1, \ldots, \overline{Z}_k$ such that $g_1, \ldots, g_{n-k}, \overline{Z}_1, \ldots, \overline{Z}_k$ forms and independent and commuting set.
- $\overline{Z}_i$ play the role of a logical pauli $Z$ operator on qubit $i$.
- The logical basis state $|x_1, \ldots, x_k\rangle_L$ is defined to be the state with stabilizer
  \[ \langle g_1, \ldots, g_{n-k}, (-1)^{x_1} \overline{Z}_1, \ldots, (-1)^{x_k} \overline{Z}_k \rangle \]
- Choose operators $\overline{X}_j$ which sends $\overline{Z}_j$ to $-\overline{Z}_j$ and leaves all other $Z_i$ and $g_i$ alone under conjugation.
- $\overline{X}_j$ has the effect of a quantum NOT gate acting on the $j$-th encoded qubit.
- Since $\overline{X}_j g_k \overline{X}_j^\dagger = g_k$, we have $\overline{X}_j g_k = g_k \overline{X}_j$. 
Suppose $C(S)$ is a stabilizer code corrupted by an error $E \in G_n$. 
Suppose $C(S)$ is a stabilizer code corrupted by an error $E \in G_n$.

- If $E$ anticommutes with an element of the stabilizer then $E$ takes $C(S)$ to an orthogonal subspace.
Suppose $C(S)$ is a stabilizer code corrupted by an error $E \in G_n$. If $E$ anticommutes with an element of the stabilizer then $E$ takes $C(S)$ to an orthogonal subspace. Thus $E$ can in principle be detected.
Suppose $C(S)$ is a stabilizer code corrupted by an error $E \in G_n$.

If $E$ anticommutes with an element of the stabilizer then $E$ takes $C(S)$ to an orthogonal subspace.

Thus $E$ can in principle be detected.

If $E \in S$ then $E$ does not corrupt the code.
Suppose $C(S)$ is a stabilizer code corrupted by an error $E \in G_n$.

If $E$ anticommutes with an element of the stabilizer then $E$ takes $C(S)$ to an orthogonal subspace.

Thus $E$ can in principle be detected

If $E \in S$ then $E$ does not corrupt the code.

If $E$ commutes with all elements of $S$ but it is not in $S$ then nothing can be done.
Suppose $C(S)$ is a stabilizer code corrupted by an error $E \in G_n$.

If $E$ anticommutes with an element of the stabilizer then $E$ takes $C(S)$ to an orthogonal subspace.

Thus $E$ can in principle be detected.

If $E \in S$ then $E$ does not corrupt the code.

If $E$ commutes with all elements of $S$ but it is not in $S$ then nothing can be done.

The set of all such $E$’s that commutes with each element of $S$ is called the centralizer of $S$, or $Z(S)$, which in this case is equal to the normalizer of $S$, i.e., the set of all $E$’s such that $EgE^\dagger \in S$ for all $g \in S$. 

\[ S \subseteq N(S) \text{ for any subgroup } S \text{ of } G_n. \]

\[ N(S) = Z(S) \text{ for any subgroup } S \text{ of } G_n \text{ not containing } -I. \]
Suppose $C(S)$ is a stabilizer code corrupted by an error $E \in G_n$.

- If $E$ anticommutes with an element of the stabilizer then $E$ takes $C(S)$ to an orthogonal subspace.
- Thus $E$ can in principle be detected.
- If $E \in S$ then $E$ does not corrupt the code.
- If $E$ commutes with all elements of $S$ but it is not in $S$ then nothing can be done.

The set of all such $E$’s that commutes with each element of $S$ is called the centralizer of $S$, or $Z(S)$, which in this case is equal to the normalizer of $S$, i.e., the set of all $E$’s such that $EgE^\dagger \in S$ for all $g \in S$.

- $S \subseteq N(S)$ for any subgroup $S$ of $G_n$. 
Suppose $C(S)$ is a stabilizer code corrupted by an error $E \in G_n$.

- If $E$ anticommutes with an element of the stabilizer then $E$ takes $C(S)$ to an orthogonal subspace.
- Thus $E$ can in principle be detected.
- If $E \in S$ then $E$ does not corrupt the code.
- If $E$ commutes with all elements of $S$ but it is not in $S$ then nothing can be done.

The set of all such $E$’s that commutes with each element of $S$ is called the centralizer of $S$, or $Z(S)$, which in this case is equal to the normalizer of $S$, i.e., the set of all $E$’s such that $EgE^\dagger \in S$ for all $g \in S$.

- $S \subseteq N(S)$ for any subgroup $S$ of $G_n$.
- $N(S) = Z(S)$ for any subgroup $S$ of $G_n$ not containing $-I$. 
Error correction conditions

- Let $S$ be the stabilizer for a stabilizer code $C(S)$
Error correction conditions

- Let $S$ be the stabilizer for a stabilizer code $C(S)$
- Let $\{E_j\}$ be a set of operation in $G_n$ such that $E_j^\dagger E_k \notin N(S) - S$ for all $j, k$. 
Error correction conditions

- Let $S$ be the stabilizer for a stabilizer code $C(S)$.
- Let $\{E_j\}$ be a set of operation in $G_n$ such that $E_j^\dagger E_k \notin N(S) - S$ for all $j, k$.
- Then $\{E_j\}$ is a correctable set of errors for the code $C(S)$. 
Error correction conditions

- Let $S$ be the stabilizer for a stabilizer code $C(S)$
- Let $\{E_j\}$ be a set of operation in $G_n$ such that $E_j^\dagger E_k \not\in N(S) - S$ for all $j, k$.
- Then $\{E_j\}$ is a correctable set of errors for the code $C(S)$.
- Let $P$ be the projector onto the code space $C(S)$
Error correction conditions

- Let $S$ be the stabilizer for a stabilizer code $C(S)$
- Let $\{E_j\}$ be a set of operation in $G_n$ such that $E_j^\dagger E_k \notin N(S) - S$ for all $j, k$.
- Then $\{E_j\}$ is a correctable set of errors for the code $C(S)$.
- Let $P$ be the projector onto the code space $C(S)$
- For given $j$ and $k$, there are two possibilities:
Error correction conditions

- Let $S$ be the stabilizer for a stabilizer code $C(S)$
- Let $\{E_j\}$ be a set of operation in $G_n$ such that $E_j^\dagger E_k \notin N(S) - S$ for all $j, k$.
- Then $\{E_j\}$ is a correctable set of errors for the code $C(S)$.
- Let $P$ be the projector onto the code space $C(S)$
- For given $j$ and $k$, there are two possibilities:
  1. $E_j^\dagger E_k \in S$
Stabilizer Codes

Error correction conditions

- Let $S$ be the stabilizer for a stabilizer code $C(S)$
- Let $\{E_j\}$ be a set of operation in $G_n$ such that $E_j^\dagger E_k \notin N(S) - S$ for all $j, k$.
- Then $\{E_j\}$ is a correctable set of errors for the code $C(S)$.

- Let $P$ be the projector onto the code space $C(S)$
- For given $j$ and $k$, there are two possibilities:
  1. $E_j^\dagger E_k \in S$
     - Then $PE_j^\dagger E_k P = P$ since $P$ is invariant under multiplication by elements of $S$. 
  2. $E_j^\dagger E_k \in G_n - N(S)$

Error correction conditions

- Let $S$ be the stabilizer for a stabilizer code $C(S)$
- Let $\{E_j\}$ be a set of operation in $G_n$ such that $E_j^\dagger E_k \not\in N(S) - S$ for all $j, k$.
- Then $\{E_j\}$ is a correctable set of errors for the code $C(S)$.
- Let $P$ be the projector onto the code space $C(S)$.
- For given $j$ and $k$, there are two possibilities:
  1. $E_j^\dagger E_k \in S$
     - Then $PE_j^\dagger E_k P = P$ since $P$ is invariant under multiplication by elements of $S$.
  2. $E_j^\dagger E_k$ in $G_n - N(S)$
Error correction conditions

- Let $S$ be the stabilizer for a stabilizer code $C(S)$
- Let $\{E_j\}$ be a set of operation in $G_n$ such that $E_j^\dagger E_k \notin N(S) - S$ for all $j, k$.
- Then $\{E_j\}$ is a correctable set of errors for the code $C(S)$.
- Let $P$ be the projector onto the code space $C(S)$
- For given $j$ and $k$, there are two possibilities:
  1. $E_j^\dagger E_k \in S$
     - Then $PE_j^\dagger E_k P = P$ since $P$ is invariant under multiplication by elements of $S$.
  2. $E_j^\dagger E_k$ in $G_n - N(S)$
     - then $E_j^\dagger E_k$ must anticommute with some element $g_l$ of $S$
Error correction conditions

- Let $S$ be the stabilizer for a stabilizer code $C(S)$
- Let $\{E_j\}$ be a set of operation in $G_n$ such that $E_j^\dagger E_k \notin N(S) - S$ for all $j, k$.
- Then $\{E_j\}$ is a correctable set of errors for the code $C(S)$.
- Let $P$ be the projector onto the code space $C(S)$
- For given $j$ and $k$, there are two possibilities:
  1. $E_j^\dagger E_k \in S$
     - Then $P E_j^\dagger E_k P = P$ since $P$ is invariant under multiplication by elements of $S$.
  2. $E_j^\dagger E_k$ in $G_n - N(S)$
     - then $E_j^\dagger E_k$ must anticommute with some element $g_l$ of $S$
     - Let $g_1, ..., g_{n-k}$ be a set of generators of $S$ so that $P = \prod_{l=1}^{n-k} (I + g_l) / 2^{n-k}$
Stabilizer Codes

Error correction conditions

- Let $S$ be the stabilizer for a stabilizer code $C(S)$
- Let $\{E_j\}$ be a set of operation in $G_n$ such that $E_j^\dagger E_k \notin N(S) - S$ for all $j, k$.
- Then $\{E_j\}$ is a correctable set of errors for the code $C(S)$.
- Let $P$ be the projector onto the code space $C(S)$.
- For given $j$ and $k$, there are two possibilities:
  1. $E_j^\dagger E_k \in S$
     - Then $PE_j^\dagger E_k P = P$ since $P$ is invariant under multiplication by elements of $S$.
  2. $E_j^\dagger E_k$ in $G_n - N(S)$
     - then $E_j^\dagger E_k$ must anticommute with some element $g_l$ of $S$
     - Let $g_1, \ldots, g_{n-k}$ be a set of generators of $S$ so that $P = \prod_{l=1}^{n-k} (I + g_l) 2^{n-k}$
     - Using the anti-commutativity gives $E_j^\dagger E_k P = (I - g_1)E_j^\dagger E_k \prod_{l=2}^{n-k} (I + g_l) 2^{n-k}$
Error correction conditions

- Let $S$ be the stabilizer for a stabilizer code $C(S)$.
- Let $\{E_j\}$ be a set of operation in $G_n$ such that $E_j^\dagger E_k \notin N(S) - S$ for all $j, k$.
- Then $\{E_j\}$ is a correctable set of errors for the code $C(S)$.
- Let $P$ be the projector onto the code space $C(S)$.
- For given $j$ and $k$, there are two possibilities:
  1. $E_j^\dagger E_k \in S$
     - Then $PE_j^\dagger E_k P = P$ since $P$ is invariant under multiplication by elements of $S$.
  2. $E_j^\dagger E_k$ in $G_n - N(S)$
     - then $E_j^\dagger E_k$ must anticommute with some element $g_l$ of $S$
     - Let $g_1, ..., g_{n-k}$ be a set of generators of $S$ so that $P = \prod_{l=1}^{n-k} (I + g_l) \frac{2n-k}{2^{n-k}}$
     - Using the anti-commutativity gives $E_j^\dagger E_k P = (I - g_1)E_j^\dagger E_k \frac{\prod_{l=2}^{n-k} (I + g_l)}{2^{n-k}}$
     - But $P(I - g_l) = 0$ since $(I + g_1)(I - g_1) = 0$. 
Error correction conditions

- Let $S$ be the stabilizer for a stabilizer code $C(S)$.
- Let $\{E_j\}$ be a set of operation in $G_n$ such that $E_j^\dagger E_k \notin N(S) - S$ for all $j, k$.
- Then $\{E_j\}$ is a correctable set of errors for the code $C(S)$.
- Let $P$ be the projector onto the code space $C(S)$.
- For given $j$ and $k$, there are two possibilities:
  1. $E_j^\dagger E_k \in S$
     - Then $P E_j^\dagger E_k P = P$ since $P$ is invariant under multiplication by elements of $S$.
  2. $E_j^\dagger E_k \in G_n - N(S)$
     - then $E_j^\dagger E_k$ must anticommute with some element $g_l$ of $S$
     - Let $g_1, \ldots, g_{n-k}$ be a set of generators of $S$ so that $P = \frac{\prod_{l=1}^{n-k}(I + g_l)}{2^{n-k}}$
     - Using the anti-commutativity gives $E_j^\dagger E_k P = (I - g_1) E_j^\dagger E_k \frac{\prod_{l=2}^{n-k}(I + g_l)}{2^{n-k}}$
     - But $P(I - g_l) = 0$ since $(I + g_1)(I - g_1) = 0$.
     - Then $P E_j^\dagger E_k P = 0$ whenever $E_j^\dagger E_k \in G_n - N(S)$.
Let $g_1, \ldots, g_{n-k}$ be a set of generators for the stabilizer of an $[n, k]$ stabilizer code.
Let $g_1, \ldots, g_{n-k}$ be a set of generators for the stabilizer of an $[n, k]$ stabilizer code.

Let $\{E_j\}$ be a set of correctable errors.
Let $g_1, ..., g_{n-k}$ be a set of generators for the stabilizer of an $[n, k]$ stabilizer code.

Let $\{E_j\}$ be a set of correctable errors.

Error-detection:
Let \( g_1, \ldots, g_{n-k} \) be a set of generators for the stabilizer of an \([n, k]\) stabilizer code.

Let \( \{E_j\} \) be a set of correctable errors.

Error-detection:

- Measure the generators \( g_1, \ldots, g_{n-k} \) to obtain the syndrome.

Let $g_1, \ldots, g_{n-k}$ be a set of generators for the stabilizer of an $[n, k]$ stabilizer code.

Let $\{E_j\}$ be a set of correctable errors.

Error-detection:

- Measure the generators $g_1, \ldots, g_{n-k}$ to obtain the syndrome.
- The syndrome is simply the results $\beta_1, \ldots, \beta_{n-k}$ of the measurements.
Let $g_1, \ldots, g_{n-k}$ be a set of generators for the stabilizer of an $[n, k]$ stabilizer code.

Let $\{E_j\}$ be a set of correctable errors.

Error-detection:

- Measure the generators $g_1, \ldots, g_{n-k}$ to obtain the syndrome.
- The syndrome is simply the results $\beta_1, \ldots, \beta_{n-k}$ of the measurements.
- If the error $E_j$ occurred, then the the error syndrome is given by $\beta_l$ such that $E_j g_l E_j^\dagger = \beta_l g_l$. 

Let $g_1, \ldots, g_{n-k}$ be a set of generators for the stabilizer of an $[n, k]$ stabilizer code.

Let $\{E_j\}$ be a set of correctable errors.

Error-detection:

- Measure the generators $g_1, \ldots, g_{n-k}$ to obtain the syndrome.
- The syndrome is simply the results $\beta_1, \ldots, \beta_{n-k}$ of the measurements.
- if the error $E_j$ occurred, then the error syndrome is given by $\beta_l$ such that $E_j g_l E_j^\dagger = \beta_l g_l$.
- If $E_j$ is the only error operator having this syndrome, then apply $E_j^\dagger$ to recover.
Let $g_1, \ldots, g_{n-k}$ be a set of generators for the stabilizer of an $[n, k]$ stabilizer code.

Let $\{E_j\}$ be a set of correctable errors.

Error-detection:

- Measure the generators $g_1, \ldots, g_{n-k}$ to obtain the syndrome.
- The syndrome is simply the results $\beta_1, \ldots, \beta_{n-k}$ of the measurements.
- If the error $E_j$ occurred, then the error syndrome is given by $\beta_l$ such that $E_j g_l E_j^\dagger = \beta_l g_l$.
- If $E_j$ is the only error operator having this syndrome, then apply $E_j^\dagger$ to recover.
- If there distinct errors $E_j$ and $E_{j'}$ such that $E_j g_l E_j^\dagger = \beta_l g_l = E_{j'} g_l E_{j'}^\dagger$, then $E_j P E_j^\dagger = E_{j'} P E_{j'}^\dagger$, where $P$ is the projector onto the code space, so $E_j^\dagger E_{j'} PE_{j'}^\dagger E_j = P$. 
Distance for a quantum Code:

- The weight of an error $E \in G_n$ is the number of terms in the tensor product which are not equal to the identity.
Distance for a quantum Code:

- The weight of an error $E \in G_n$ is the number of terms in the tensor product which are not equal to the identity.
- The distance of a stabilizer code $C(S)$ is the minimum weight of an element of $N(S) - S$. 
Distance for a quantum Code:

- The weight of an error $E \in G_n$ is the number of terms in the tensor product which are not equal to the identity.
- The distance of a stabilizer code $C(S)$ is the minimum weight of an element of $N(S) - S$.
- If $C(S)$ is an $[n, k]$ code with distance $d$ then we say that $C(S)$ is an $[n, k, d]$ stabilizer code.
Distance for a quantum Code:

- The weight of an error $E \in G_n$ is the number of terms in the tensor product which are not equal to the identity.
- The distance of a stabilizer code $C(S)$ is the minimum weight of an element of $N(S) - S$.
- If $C(S)$ is an $[n, k]$ code with distance $d$ then we say that $C(S)$ is an $[n, k, d]$ stabilizer code.
- A code with distance at least $2t + 1$ is able to correct arbitrary errors on any $t$ qubits.