QUANTUM ERROR CORRECTION
Classical error correction

Example
Let us consider a symmetric binary channel with a bit flip error occurring with probability $p$.

If we use one physical bit to represent one bit of information, then the error will destroy the information with probability $p$.

But we can encode the information into several physical bits, so the error, occurring with not too high probability $p$, will not be able to flip the logical bit even if it flips some of the physical bits of the code.
Encoding using repetition code:

\[
\begin{align*}
0 & \rightarrow 000 \\
1 & \rightarrow 111
\end{align*}
\]

For example, after sending the logical qubit through the channel, we get 100 as the output. For small \( p \), we can conclude that the first bit was flipped and that the input bit was 0.

The probability that two or more bits are flipped is

\[
p_{\text{error}} = 3p^2(1 - p) + p^3 = 3p^2 - 2p^3
\]

If \( p < 1/2 \) then the encoded information is transmitted more reliably: \( p_{\text{error}} < p \).
Quantum error correction

Quantum information faces some nontrivial difficulties which have no analog in classical information processing:

1) **No-cloning**: duplicating quantum states to get repetition code is impossible.

2) **Errors are continuous**: a continuum of different errors can occur on a single qubit; determining which error occurred in order to correct it would require infinite precision (i.e. resources).

3) **Measurement destroys quantum information**: Classical information can be observed without destroying it and then decoded, but quantum information is destroyed by measurement and can not be recovered.

Despite these difficulties, **quantum error correction** is possible.
Three qubit bit flip code: encoding

Let us consider a symmetric binary quantum channel with a quantum bit flip error, $X$, occurring with probability $p$.

Encoding of a qubit $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ using the repetition code:

$|0\rangle \rightarrow |0_L\rangle = |000\rangle$

$|1\rangle \rightarrow |1_L\rangle = |111\rangle$

$|\psi\rangle \rightarrow |\psi_L\rangle = c_0|000\rangle + c_1|111\rangle$
Three qubit bit flip code: error detection

We need to measure what error occurred on the quantum state, that is, **error syndrome**. For bit flip error there are four error syndroms corresponding to the projectors:

\[
P_0 = |000\rangle\langle 000| + |111\rangle\langle 111| \quad \text{no error}
\]

\[
P_1 = |100\rangle\langle 100| + |011\rangle\langle 011| \quad \text{bit flip error on first qubit}
\]

\[
P_2 = |010\rangle\langle 010| + |101\rangle\langle 101| \quad \text{bit flip error on second qubit}
\]

\[
P_3 = |001\rangle\langle 001| + |110\rangle\langle 110| \quad \text{bit flip error on third qubit}
\]

Assuming the error happens on the first qubit, so the corrupted state is

\[
|\psi\rangle = c_0|100\rangle + c_1|011\rangle
\]

then \(\langle \psi|P_1|\psi\rangle = 1\) reveals that the bit flip occurred on the first qubit. However, it does not destroy the qubit superposition, so we learn only about where error occurred but no information about the state itself.
Three qubit bit flip code: recovery

Error syndrome is used to recover the original quantum state.

In our example, the error syndrome implies we need to apply bit flip on the first qubit to correct the error.

Similarly, other syndromes imply different recovery procedure.
Three qubit bit flip code: fidelity analysis

Error analysis:

The error correction works perfectly, if bit flips occur on at most one of the three qubits.

The probability of an error which remains uncorrected is then $3p^2 - 2p^3$, like in the classical case.

However, the effect of an error on a state depends on the state also. To analyze the errors properly, we use the **fidelity**.
Example:

The objective (of the error correction) is to increase the minimal fidelity to its maximum. Suppose the bit flip error channel, and $|\psi\rangle$ as the state of interest.

**Without using the error correcting code:** the state after the error channel is

$$\rho = (1 - p) |\psi\rangle\langle\psi| + p X|\psi\rangle\langle\psi|X$$

and the fidelity is

$$F_0 = \sqrt{\langle\psi|\rho|\psi\rangle} = \sqrt{(1 - p) + p \langle\psi|X|\psi\rangle\langle\psi|X|\psi\rangle}$$

since the second term is nonnegative and equals to zero for $|\psi\rangle = |0\rangle$ the minimum fidelity is $F_0 = \sqrt{1 - p}$. 
With using the three qubit bit flip code: the state after the error channel is

\[ [(1 - p)^3 + 3p(1 - p)^2] \rho + \ldots \]

and the fidelity is

\[ F_{EC} = \sqrt{\langle \psi | \rho | \psi \rangle} \geq \sqrt{(1 - p)^3 + 3p(1 - p)^2} = \sqrt{1 - 3p^2 + 2p^3} \]

so the fidelity is improved by using the error correcting code provided \( p < 1/2 \).

For example, if the error probability is 0.2 then the fidelities are respectively

\[ F_0 = 0.89 \]
\[ F_{EC} = 0.98 \]
Three qubit bit flip code: towards generalization

A different look at syndrome measurement: Instead of measuring the projectors $P_0$, $P_1$, $P_2$, and $P_3$, we perform two measurements of the following observables

$$Z_1 Z_2 = Z \otimes Z \otimes I \quad Z_2 Z_3 = I \otimes Z \otimes Z$$

Each of these observables has eigenvalue $+1$ and $-1$, so both measurements provide the total of two bits of information, that is four possible syndromes, without revealing the qubit state, i.e. without collapsing the state.
The first measurement, $Z_1Z_2$, can be seen as comparing whether the first and second qubit are the same; the spectral decomposition

$$Z_1Z_2 = (|00\rangle\langle00| + |11\rangle\langle11|) \otimes I - (|01\rangle\langle01| + |10\rangle\langle10|) \otimes I$$

shows that this observable corresponds to two projective measurements with eigenvalue $+1$ if both qubits are the same or $-1$ if they are different.

Similarly, $Z_2Z_3$ compares values of the second and third qubit.

By combining both measurements, we can determine where the error occurred:

- $Z_1Z_2 = +1$ $Z_2Z_3 = +1$ no error
- $Z_1Z_2 = -1$ $Z_2Z_3 = +1$ bit flip error on first qubit
- $Z_1Z_2 = -1$ $Z_2Z_3 = -1$ bit flip error on second qubit
- $Z_1Z_2 = +1$ $Z_2Z_3 = -1$ bit flip error on third qubit
Three qubit phase flip code: encoding

This error channel flips the relative phase between $|0\rangle$ and $|1\rangle$ with probability $p$ and is given by the quantum operation

$$|\psi\rangle\langle\psi| \rightarrow \rho = (1 - p) |\psi\rangle\langle\psi| + p Z|\psi\rangle\langle\psi|Z$$

We know that $HZH = X$, where $H$ is the Hadamard gate. That is the phase flip acts as the bit flip in the basis

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|−\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
This suggests that the following encoding of a qubit $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ is appropriate for the phase flip error

$|0\rangle \quad \rightarrow \quad |0_L\rangle = |++\rangle$

$|1\rangle \quad \rightarrow \quad |1_L\rangle = |--\rangle$

$|\psi\rangle \quad \rightarrow \quad |\psi_L\rangle = c_0|++\rangle + c_1|--\rangle$
Three qubit phase flip code: error detection

Error is detected using the same projective measurements as for the bit flip error
detection conjugated with Hadamard rotations:

\[ \tilde{P}_j = H^\otimes 3 P_j H^\otimes 3 \]

Alternatively, the syndrome measurements can be performed using the observables

\[ H^\otimes 3 Z_1 Z_2 H^\otimes 3 = X_1 X_2 \quad H^\otimes 3 Z_2 Z_3 H^\otimes 3 = X_2 X_3 \]

Measurement of these observables corresponds to comparing the signs of qubits,
for example \( X_1 X_2 \) gives the eigenvalue \(+1\) for \( |+\> \otimes |.> \) and \( |--\> \otimes |.> \), and the
eigenvalue \(-1\) for \( |+\> \otimes |.> \) and \( |--\> \otimes |.> \).
Three qubit phase flip code: recovery

Error correction is completed with the recovery operation, which is the Hadamard conjugated recovery operation of the bit flip code.

For example, if the phase flip, that is the flip from $|+\rangle$ and $|−\rangle$ and vice versa, was detected on the second qubit, then the recovery operation is $H X_2 \ H = Z_2$.

Remark:
This code for the phase flip channel obviously has the same characteristics, i.e. the minimum fidelity etc., as the code for the bit flip channel. These two codes are unitarily equivalent, that is, they are related to each other by a unitary transformation.
Three qubit phase flip code: example

The phase flip error creates a mixed state

$$\rho = (1 - 3p) |\psi_L\rangle\langle\psi_L| + p Z_1 |\psi_L\rangle\langle\psi_L| Z_1 + p Z_2 |\psi_L\rangle\langle\psi_L| Z_2 + p Z_3 |\psi_L\rangle\langle\psi_L| Z_3$$

from the original encoded pure state

$$|\psi_L\rangle = c_0 |++\rangle + c_1 |--\rangle$$

Error syndrome measurement using the observables $X_1X_2$ and $X_2X_3$ yields the eigenvalues $-1$ and $-1$ and collapses the mixed state into the pure state with the phase error on the second qubit

$$|\psi'_L\rangle = c_0 |+-\rangle + c_1 |-\rangle$$

The original state can now be recovered by applying the phase flip $Z_2$. 
The Shor nine-qubit code

This code protects against arbitrary error on a single qubit. It is a concatenation of the three qubit bit flip code and three qubit phase flip code

\[
|0_L\rangle = \frac{1}{\sqrt{2^3}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)
\]

\[
|1_L\rangle = \frac{1}{\sqrt{2^3}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)
\]

The qubit is first encoded using the phase flip code and then it is encoded using the bit flip code. The result is the nine qubit Shor code.
The Shor code: bit flip error

The encoded single qubit state is given as

\[
|\psi_L\rangle = \frac{c_0}{\sqrt{2^3}} (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \\
+ \frac{c_1}{\sqrt{2^3}} (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)
\]

Let us assume that the bit flip error happens on the 4th qubit, so the resulting state after the syndrome measurement would be

\[
|\psi'_L\rangle = \frac{c_0}{\sqrt{2^3}} (|000\rangle + |111\rangle) \otimes (|100\rangle + |011\rangle) \otimes (|000\rangle + |111\rangle) \\
+ \frac{c_1}{\sqrt{2^3}} (|000\rangle - |111\rangle) \otimes (|100\rangle - |011\rangle) \otimes (|000\rangle - |111\rangle)
\]
Error syndromes are all obtained by measuring the following six observables

\[ Z_1Z_2 \quad Z_2Z_3 \quad Z_4Z_5 \quad Z_5Z_6 \quad Z_7Z_8 \quad Z_8Z_9 \]

which detect the bit string parity of neighboring pair of qubits on each of the three-qubit blocks. The result in our example is

\[ +1 \quad +1 \quad -1 \quad +1 \quad +1 \quad +1 \]

and thus indicates that the bit flip error happened on the fourth qubit, that is, the first qubit of the second block.

The original state is recovered by applying the bit flip \( X_4 \).
The Shor code: phase flip error

The encoded single qubit state is given as

$$|\psi_L\rangle = \frac{c_0}{\sqrt{2^3}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$+ \frac{c_1}{\sqrt{2^3}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$

Let us assume that the phase flip error happens on the 4th qubit, so the resulting state after the syndrome measurement would be

$$|\psi'_L\rangle = \frac{c_0}{\sqrt{2^3}}(|000\rangle + |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$+ \frac{c_1}{\sqrt{2^3}}(|000\rangle - |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle - |111\rangle)$$
Error syndrom measurements have to identify on which three-qubit block the phase flip happened. The relevant set of the phase flip syndromes is obtained by measuring the following two observables:

$$X_1X_2X_3X_4X_5X_6 \quad X_4X_5X_6X_7X_8X_9$$

which together detect on which three qubit block the error occurred. The result in our example is

$$-1 \quad -1$$

and thus indicates that the phase flip error happened on the second block.

The original state is recovered by applying the phase flip to each qubit of the second block:

$$Z_4Z_5Z_6$$
Classical linear codes: encoding

A linear code $C$ encoding $k$ bits of information into a $n$ bit code space is specified by $n \times k$ generating matrix $G$ whose entries are elements of $\mathbb{Z}_2 = \{0, 1\}$. A message $x$ is encoded as

$$x \rightarrow y = Gx \mod 2$$

A code that uses $n$ bits to encode $k$ bits of information is an $[n, k]$ code. A linear code $[n, k]$ requires only $kn$ bits of the generating matrix $G$.

Example:

Three bit repetition code is a $[3, 1]$ code with the generating matrix $G$:

$$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad G(0) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = (000)^T \quad G(1) = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = (111)^T$$
Classical linear codes: error detection

We introduce the **parity check matrix** $H$ that is $(n - k) \times n$ matrix such that an $[n, k]$ code is defined by all $n$ element vectors that form the kernel of $H$

$$H y = 0$$

Example: $[3, 1]$ repetition code:

Pick $3 - 1 = 2$ linearly independent vectors orthogonal to the columns of $G$, that is $(110)^T$ and $(011)^T$ and define the parity check matrix as

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

The codewords $(000)^T$ and $(111)^T$ are the only vectors in the kernel of $H$. Let us consider the output of a noisy channel to be $y' = y + e = (100)^T$. The parity check matrix would reveal the error syndrome $H y' = H(y + e) = He = (10)^T$. 

Distance measures for codes

The Hamming distance $d(x, y)$ between the codewords $x$ and $y$ is defined to be the number of places at which $x$ and $y$ differ: e.g. $d((1, 1, 0, 0), (0, 1, 0, 1)) = 2$.

The Hamming weight of a word $x$: $wt(x) = d(0, x)$. Note: $d(x, y) = wt(x + y)$.

The distance of a code $C$: $d(C) = \min_{x, y \in C, x \neq y} d(x, y) = \min_{x \in C, x \neq 0} wt(x)$

Setting $d = d(C)$ then the code C can be described as $[n, k, d]$ code.

Important:
if $d \geq 2t + 1$ where $t \in \mathbb{Z}$, the given code can correct up to $t$ bits.
Introduction to stabilizer codes (additive codes)

Idea

\[ |\psi> = (1/2)^{1/2}(|00> + |11>) \]

\[ X_1X_2|\psi> = |\psi> \]
\[ Z_1Z_2|\psi> = |\psi> \]

|\psi> is stabilized by \( X_1X_2 \) and \( Z_1Z_2 \)

Quantum states can more easily be specified by the operators that stabilize them than working explicitly with quantum states.

Theory

The Pauli group \( G_n \) on \( n \) qubits.

Example \( G_1 \):

\( \{ \pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ \} \)

- this set forms a group under matrix multiplication

Definition:

Suppose \( S \) is a subgroup of \( G_n \) and let \( V_S \) be the set of \( n \) qubit states which are fixed by every element of \( S \). \( V_S \) is a vector space stabilized by \( S \), and \( S \) is said to be the stabilizer of the space \( V_S \).
Introduction to stabilizer codes

Definition:
Suppose $S$ is a subgroup of $G_n$ and let $V_S$ be the set of $n$ qubit states which are fixed by every element of $S$. $V_S$ is a vector space stabilized by $S$, and $S$ is said to be the stabilizer of the space $V_S$.

Example:
$n=3$ qubits and $S = \{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$
The subspace stabilized by: $Z_1Z_2$ is spanned by $\{|000>, |001>, |110>, |111>\}$.
$Z_2Z_3$ is spanned by $\{|000>, |100>, |011>, |111>\}$.
$Z_1Z_3$ is spanned by $\{|000>, |010>, |101>, |111>\}$.

The elements $|000>$ and $|111>$ are fixed by all the operators, so $V_s$ is spanned by these states.
Clearly we can work with only two of the operators because e.g.
$Z_1Z_3 = (Z_1Z_2)(Z_2Z_3)$, and $(Z_1Z_2)^2 = I$.
The description in terms of these generators is convenient because we only need to show that the states are stabilized by the generators:

in this example, $S = <Z_1Z_2, Z_2Z_3>$.

What subgroup $S$ of the Pauli group can be used as the stabilizer for a nontrivial $V_S$?
- two conditions need to be satisfied: (a) the elements of $S$ commute;
  (b) $-I$ is not an element of $S$. 
Error correction using stabilizer codes

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, and the error can in principle be detected by projective measurement.

If $E \in S$, then $E$ does not corrupt the state at all.

But the problem emerges from possibility that $E$ commutes with all elements of $S$, but $E \not\in S$, i.e. $Eg = gE$ for all $g \in S$.

Centralizer $Z(S)$: the set $E \in G_n$ s.t. $Eg = gE$ all $g \in S$.

Normalizer $N(S)$: the set $E \in G_n$ s.t. $EgE^+ \in S$;
- for any subgroup $S$ of $G$ not containing $-I$, $N(S) = Z(S)$.

Theorem:
Let $S$ be the stabilizer for a stabilizer code $C(S)$. Suppose $\{E_j\}$ is a set of operators in $G_n$ s.t. $E_j^+E_k \not\in N(S) – S$ for all $j$ and $k$. Then $\{E_j\}$ is a correctable set of errors for the code $C(S)$. 
Examples of stabilizer codes

Theorem:
Let S be the stabilizer for a stabilizer code C(S). Suppose \{E_j\} is a set of operators in G_n s.t. E_j^*E_k \not\in N(S) – S for all j and k. Then \{E_j\} is a correctable set of errors for the code C(S).

1) Three qubit bit flip code
is spanned by |000\> and |111\> with the stabilizer generated by \(Z_1Z_2\) and \(Z_2Z_3\).

The error set is \{I, X_1, X_2, X_3\}

It is easy to show explicitly that every possible product of two elements of this set anticommutes with the stabilizer (except for I which is the element of S), so thus by the theorem above the error set forms a correctable set for the three qubit Bit flip code with the stabilizer \(S = <Z_1Z_2, Z_2Z_3>\).

Error detection is carried by measuring the stabilizer generators.

If for example, the error \(X_1\) occurred, then the stabilizer is transformed into \(<-Z_1Z_2, Z_2Z_3>\), so the syndrom measurement gives the result -1 and +1. Similarly the error \(X_2\) gives syndromes -1 and -1, and \(X_3\) gives +1 and -1.

The original state is recovered by applying the inverse operation to the error Indicated by the error syndrome.
Examples of stabilizer codes

2) Shor's nine-qubit code

\[ |0\rangle \rightarrow |0_L\rangle = (1/2)^{3/2}[(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)] \]

\[ |1\rangle \rightarrow |1_L\rangle = (1/2)^{3/2}[(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)] \]

Stabilizer generators

\begin{align*}
g_1 & : Z Z I I I I I I I \\
g_2 & : I Z Z I I I I I I \\
g_3 & : I I I Z Z I I I I \\
g_4 & : I I I I Z Z I I I \\
g_5 & : I I I I I I I Z Z \\
g_6 & : I I I I I I Z Z \\
g_7 & : X X X X X X X I I I \\
g_8 & : I I I X X X X X \\
\end{align*}

It is easy to check that all single qubit errors form a correctable set of errors for this code.

For example, consider the errors \(X_1\) and \(Y_4\). Their product \(X_1Y_4\) anticommutes with \(Z_1Z_2\) and thus is not in \(N(S)\). Similarly, all other products of two errors from the error set of all single qubit errors for this code anticommute with at least one element of the stabilizer \(S\), and thus are not in \(N(S)\).

This implies that the Shor code can be used to correct an arbitrary single qubit error.

Homework: Show that the encoded Z and X operations over the Shor code are realized by the operators \(X_1X_2X_3X_4X_5X_6X_7X_8X_9\) and \(Z_1Z_2Z_3Z_4Z_5Z_6Z_7Z_8Z_9\) respectively.
Examples of stabilizer codes

3) Steane [7,1] code

|0> → |0_L> = (1/2)^3/2(|0000000>+|1010101>+|0110011>+|1100110>+
+ |0001111>+|1011010>+|0111100>+|1101001>)

|1> → |1_L> = (1/2)^3/2(|1111111>+|01010101>+|1001100>+|0011001>+
+ |1110000>+|0100101>+|1000011>+|0010110>)

To construct the stabilizer generators for a CSS(C_1,C_2) code, we first introduce a check matrix, which for CSS codes is formed as

\[
\begin{pmatrix}
H(C_2) & 0 \\
0 & H(C_1)
\end{pmatrix}
\]

The rows of this matrix correspond to the stabilizer generators g_1, ..., g_l; the left side of the matrix contains “1”s to indicate which generators contain Xs, and the right side contains “1”s to indicate which generators contain Zs. (In general case, the presence of “1”s on both sides indicates Ys in the generator.)

Example

the check matrix of the Steane code

| C_1 = C |
| C_2 = C^\perp |

\[
\begin{bmatrix}
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1
\end{bmatrix}
\]
Examples of stabilizer codes

Steane [7,1] code

\[|0\rangle \rightarrow |0_L\rangle = (1/2)^{3/2}(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0011111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle)\]

\[|1\rangle \rightarrow |1_L\rangle = (1/2)^{3/2}(|1111111\rangle + |01010101\rangle + |1001100\rangle + |0011001\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle)\]

Stabilizer generators

\[
g_1 = \begin{bmatrix} I & I & I & X & X & X & X \end{bmatrix} \\
g_2 = \begin{bmatrix} I & X & X & I & I & X & X \end{bmatrix} \\
g_3 = \begin{bmatrix} X & I & X & I & X & I & X \end{bmatrix} \\
g_4 = \begin{bmatrix} I & I & I & Z & Z & Z & Z \end{bmatrix} \\
g_5 = \begin{bmatrix} I & Z & Z & I & I & Z & Z \end{bmatrix} \\
g_6 = \begin{bmatrix} Z & I & Z & I & Z & I & Z \end{bmatrix}
\]

It is easy to check that all single qubit errors form a correctable set of errors for the Steane code, implying that this code can be used to correct an arbitrary single qubit error.

Encode operations

\[
X_e = X_1X_2X_3X_4X_5X_6X_7 \\
Z_e = Z_1Z_2Z_3Z_4Z_5Z_6Z_7
\]
Fault-tolerant quantum computation

Reliable quantum computation can be achieved even with faulty gates provided the error probability per gate is below certain threshold.

To perform quantum computation directly on encoded quantum states, we replace an original quantum circuit by encoded circuit, i.e. each qubit by encoded qubit using e.g. the Steane code, and each operation by the appropriate encoded operation. This is not enough for fault-tolerance.

Problems:
1) Encoded gates can cause errors to propagate;
2) The encoded CNOT can cause an error on encoded control qubit to spread to an encoded target qubit.

Fault-tolerant encoded operations are those which ensure that a failure anywhere during the computation can only propagate to a small number of qubits in each block of the encoded data, so that error correction can effectively remove it.

We define the fault-tolerance of a procedure to be the property that if only one component in the procedure fails then the failure causes at most one error in each encoded block of qubits output from the procedure.
Concatenated codes and threshold

A fault tolerant CNOT gate

The procedure introduces two errors into the 1st encoded block with probability $O(p^2)$.

Concatenated codes and the threshold theorem

A quantum circuit containing $p(n)$ gates may be simulated with probability of error at most $\varepsilon$ using $O(poly(\log p(n)/\varepsilon)p(n))$ gates on hardware whose components fail with probability at most $p$, provided $p$ is below some constant threshold, $p < p_{th}$, and given reasonable assumptions about the noise in the underlying hardware.

The typical thresholds are $p_{th} \sim 10^{-4} - 10^{-5}$

i.e. allowable noise (error) is about 0.01% - too small!!!

Are there any other routes to fault-tolerant quantum computing?
Natural fault-tolerance
Quantum statistics

Configuration space of \( n \) indistinguishable particles in \( d \) dimensional space excluding diagonal points \( D \):

\[
M_n = \frac{(R^n - D)}{S_n}
\]

In (3+1) dimensions, the configuration space is simply connected; quantum mechanics permits only two kinds of statistics:

Exchanging particles in 3D space belongs to the permutation group \( S_n \):

Statistics follows from one-dimensional representations of \( S_n \):

Bose-Einstein statistics: \( \chi_+(\sigma) = +1 \)
Fermi-Dirac statistics: \( \chi_-(\sigma) = +1 \) (even) or \(-1\) (odd permutations)
Anyons

are particles with fractional statistics

The configuration space of \( n \) indistinguishable particles in 2 dimensional space excluding diagonal points is multiply connected

Exchanging particles on a plane is not anymore an element of permutation group

it is braiding, an element of a braid group!
A braid group for $n$ strands (particles) has $n$ generators $\{1, \sigma_1, \ldots, \sigma_{n-1}\}$ which satisfy:

$$\sigma_i \sigma_j = \sigma_j \sigma_i \quad \text{for } |j-i| > 1$$

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$$

One-dimensional irreps of $B_n$ correspond to abelian fractional statistics:

$$\chi_0(\sigma) = e^{i\theta} \quad \in \ U(1)$$

Higher dimensional irreps correspond to nonabelian fractional statistics:

$$\chi_0(\sigma) = e^{i\theta\Lambda} \quad \text{e.g. } \in \ SU(2)$$

Example:

$$\sigma_i$$
Topological quantum computation

- is naturally fault-tolerant
- is realized by braiding (and exciting and fusing) non-abelian anyons

Topological phase

2D quantum system

vacuum

trefoil knot

time
Topological phases of matter

- topological phases are phases of two-dimensional many-body quantum systems whose properties depend only on topology of the manifold on whose surface a given phase is realized

- their effective description is given by topological quantum field theory (3 dimensional) defined e.g. by the Chern-Simons action:

\[ S = \frac{k}{4\pi} \int_{\Gamma} dt \, dx \, dy \left( a_y \partial_t a_x - a_x \partial_t a_y \right) \]

Example: doubled SU(2)_k Chern-Simons theory (PT invariant theory):

- \( k = 1 \) - abelian topological phase - quantum memory
- \( k \geq 2 \) - non-abelian
- \( k = 3, 5 \ldots \) - non-abelian and universal - universal QC

- topological phases are invariant with local geometry and hence quantum information stored in them is invariant with local error processes
Topological phases of matter

• are ground states of certain strongly correlated many-body quantum systems
e.g. in Coulomb gauge, $a_t = 0$: $\mathcal{L} = a_y \partial_t a_x - a_x \partial_t a_y$

$$\mathcal{H} = \frac{\partial \mathcal{L}}{\partial (\partial_t a_x)} \partial_t a_x + \frac{\partial \mathcal{L}}{\partial (\partial_t a_y)} \partial_t a_y - \mathcal{L} = 0$$

• energy spectrum of matter in a topological phase is characterized by

  finite topology-dependent ground state degeneracy,
e.g. for the doubled SU(2) Chern-Simons theory: $(k+1)^{2g}$

$$= \frac{1}{n_{\text{even}}} - \frac{1}{n_{\text{odd}}}$$

spectral gap

excitations of stray anyons, which may cause
ters via non-local processes, are at sufficiently
low temperatures exponentially
suppressed due to the spectral gap !!!

Topological phases of matter in physical systems

- fractional quantum Hall systems (FQH)
  particularly promising !!!

- quantum lattice systems
  atoms in optical lattices
  polar molecules
  Josephson-junction arrays

- $p_x+ip_y$ superconductors
  Sr$_2$RuO$_4$
  Helium-3

- rotating Bose-Einstein condensates

- nuclear matter
Topological phases of matter in FQH systems

Longitudinal resistance
\[ R_{xx} = \frac{V_x}{I_x} \]

Transverse (Hall) resistance
\[ R_{xy} = \frac{V_y}{I_x} = \frac{h}{e^2} \]
- is quantized!!!

Theory
- nonabelian quantum Hall phases at \( \nu = 5/2 \) and \( 12/5 \)

Experiment
- detecting these phases in high mobility samples

Eisenstein, Stormer, Science 248, 1461 (1990)


Eisenstein, Stormer, Science 248, 1461 (1990)


Topological quantum computation in FQH systems

- non-abelian topological phases predicted in fractional quantum Hall systems at the filling $v=5/2$ and $12/5$; these have recently been detected experimentally in extremely clean samples
  

- experimental tests of fractional statistics using Laughlin interferometer
  

- relation between boundary (CFT) and bulk (TQFT) – “holographic principle”

- topologically protected qubit

Topological quantum computation

• provides new insights into quantum algorithms and complexity theory

For more information about topological quantum computation, see e.g.
• G. P. Collins: Computing with Knots, Scientific American, April 2006
PHYSICAL IMPLEMENTATIONS
DiVincenzo criteria

1) A scalable physical system with well characterized qubits

2) The ability to initialize the state of the qubits to a fiducial initial state, such as $|00\ldots0\rangle$

3) Long decoherence times, much longer than the gate operation time

4) A universal set of quantum gates

5) A qubit-specific measurement capability

Additional criteria for quantum communication

6) The ability to interconnect stationary and flying qubits

7) The ability to faithfully transmit the flying qubits between specified locations
### Physical realizations of quantum computation

<table>
<thead>
<tr>
<th>QC Approach</th>
<th>The DiVincenzo Criteria</th>
<th>QC Networkability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>#1</td>
<td>#2</td>
</tr>
<tr>
<td>NMR</td>
<td>![Green Ball]</td>
<td>![Green Ball]</td>
</tr>
<tr>
<td>Trapped Ion</td>
<td>![Green Ball]</td>
<td>![Green Ball]</td>
</tr>
<tr>
<td>Neutral Atom</td>
<td>![Green Ball]</td>
<td>![Green Ball]</td>
</tr>
<tr>
<td>Cavity QED</td>
<td>![Green Ball]</td>
<td>![Green Ball]</td>
</tr>
<tr>
<td>Optical</td>
<td>![Green Ball]</td>
<td>![Green Ball]</td>
</tr>
<tr>
<td>Superconducting</td>
<td>![Green Ball]</td>
<td>![Green Ball]</td>
</tr>
<tr>
<td><strong>Unique Qubits</strong></td>
<td><strong>This field is so diverse that it is not feasible to label the criteria with “Promise” symbols.</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Legend:**
- ![Green Ball] = a potentially viable approach has achieved sufficient proof of principle
- ![Green Ball] = a potentially viable approach has been proposed, but there has not been sufficient proof of principle
- ![Red Ball] = no viable approach is known

The column numbers correspond to the following QC criteria:

#1. A scalable physical system with well-characterized qubits.
#2. The ability to initialize the state of the qubits to a simple fiducial state.
#3. Long (relative) decoherence times, much longer than the gate operation time.
#4. A universal set of quantum gates.
#5. A qubit-specific measurement capability.
#6. The ability to interconvert stationary and flying qubits.
#7. The ability to faithfully transmit flying qubits between specified locations.

Quantum Computation Roadmap
http://qist.lanl.gov/