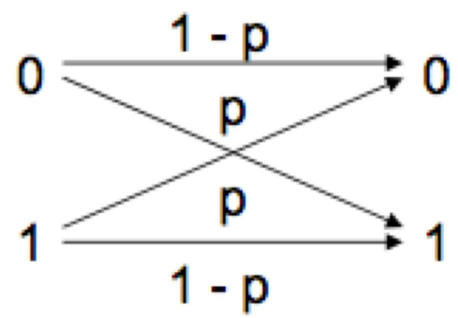
QUANTUM ERROR CORRECTION

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:

$$\begin{array}{ccc} 0 & \rightarrow & 000 \\ 1 & \rightarrow & 111 \end{array}$$

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

$$p_{error} = 3p^2(1-p) + p^3 = 3p^2 - 2p^3$$

If $p < 1/2$ then the encoded information is transmitted more reliably: $p_{error} < p$.

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.

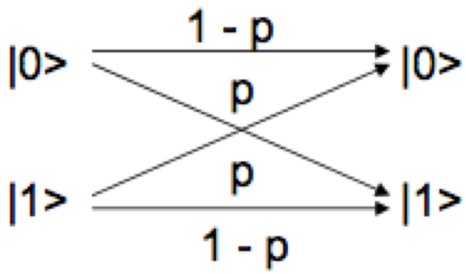
2) **Errors are continuous:** a continuum of different errors can occur on a single qubit; determining which error occurred in order to correct it would require infinite precision (i.e. resources).

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.

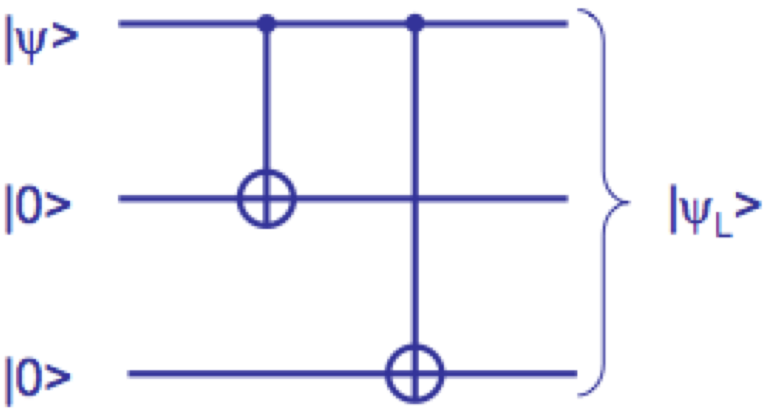
Despite these difficulties, **quantum error correction** is possible.

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:

$$
\begin{aligned}
P_0 &= |000\rangle\langle 000| + |111\rangle\langle 111| && \text{no error} \\
P_1 &= |100\rangle\langle 100| + |011\rangle\langle 011| && \text{bit flip error on first qubit} \\
P_2 &= |010\rangle\langle 010| + |101\rangle\langle 101| && \text{bit flip error on second qubit} \\
P_3 &= |001\rangle\langle 001| + |110\rangle\langle 110| && \text{bit flip error on third qubit}
\end{aligned}
$$

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

$$\begin{aligned} F_0 &= 0.89 \\ F_{EC} &= 0.98 \end{aligned}$$

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

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

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, $Z_1 Z_2$, can be seen as comparing whether the first and second qubit are the same; the spectral decomposition

$$Z_1 Z_2 = (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I - (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I$$

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

Similarly, $Z_2 Z_3$ compares values of the second and third qubit.

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

$Z_1 Z_2 = +1$	$Z_2 Z_3 = +1$	no error
$Z_1 Z_2 = -1$	$Z_2 Z_3 = +1$	bit flip error on first qubit
$Z_1 Z_2 = -1$	$Z_2 Z_3 = -1$	bit flip error on second qubit
$Z_1 Z_2 = +1$	$Z_2 Z_3 = -1$	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

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

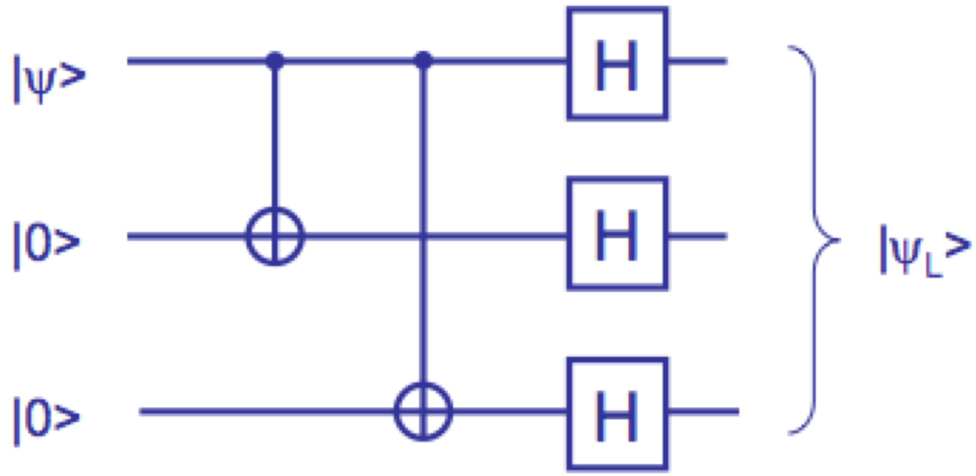
We know that $HZH = X$, where H is the Hadamard gate. That is the phase flip acts as the bit flip in the basis

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

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

$$\begin{aligned} |0\rangle \quad &\rightarrow \quad |0_L\rangle = |+++\rangle \\ |1\rangle \quad &\rightarrow \quad |1_L\rangle = |---\rangle \end{aligned}$$

$$|\psi\rangle \quad \rightarrow \quad |\psi_L\rangle = c_0|+++\rangle + c_1|---\rangle$$



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:

$$\bar{P}_j = H^{\otimes 3}\, P_j\, H^{\otimes 3}$$

Alternatively, the syndrome measurements can be performed using the observables

$$H^{\otimes 3}\, Z_1 Z_2\, H^{\otimes 3} = X_1 X_2 \qquad H^{\otimes 3}\, Z_2 Z_3\, H^{\otimes 3} = X_2 X_3$$

Measurement of these observables corresponds to comparing the signs of qubits, for example X_1X_2 gives the eigenvalue $+1$ for $|++\rangle \otimes |\,.\,\rangle$ and $|--\rangle \otimes |\,.\,\rangle$, and the eigenvalue -1 for $|+-\rangle \otimes |\,.\,\rangle$ and $|-+\rangle \otimes |\,.\,\rangle$.

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 eigen-values -1 and -1 and collapses the mixed state into the pure state with the phase error on the second qubit

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

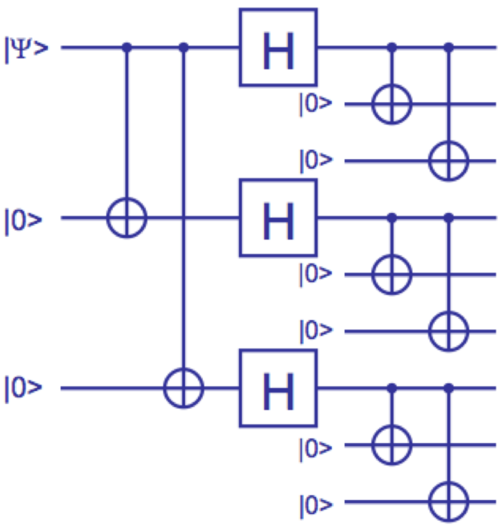
The original state can now be recovered by applying the phase flip Z_2.

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

$$
\begin{aligned}
|\psi_L\rangle &= \frac{c_0}{\sqrt{2^3}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \\
&\quad + \frac{c_1}{\sqrt{2^3}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)
\end{aligned}
$$

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

$$
\begin{aligned}
|\psi'_L\rangle &= \frac{c_0}{\sqrt{2^3}}(|000\rangle + |111\rangle) \otimes (|100\rangle + |011\rangle) \otimes (|000\rangle + |111\rangle) \\
&\quad + \frac{c_1}{\sqrt{2^3}}(|000\rangle - |111\rangle) \otimes (|100\rangle - |011\rangle) \otimes (|000\rangle - |111\rangle)
\end{aligned}
$$

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

$$+1 \qquad +1 \qquad -1 \qquad +1 \qquad +1 \qquad +1$$

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

$$
\begin{aligned}
|\psi_L\rangle &= \frac{c_0}{\sqrt{2^3}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \\
&\quad + \frac{c_1}{\sqrt{2^3}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)
\end{aligned}
$$

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

$$
\begin{aligned}
|\psi_L'\rangle &= \frac{c_0}{\sqrt{2^3}}(|000\rangle + |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle + |111\rangle) \\
&\quad + \frac{c_1}{\sqrt{2^3}}(|000\rangle - |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle - |111\rangle)
\end{aligned}
$$

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:

$$X_1X_2X_3X_4X_5X_6 \qquad X_4X_5X_6X_7X_8X_9$$

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

$$-1 \qquad -1$$

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

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

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:

$$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \qquad G(0) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = (000)^T \qquad G(1) = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = (111)^T$$

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

$$Hy = 0$$

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 $Hy' = H(y+e) = He = (10)^T$.

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. $d((1100), (0101)) = 2$.

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

Quantum states can easily be specified by the operators that stabilize them. For example

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$\left.\begin{aligned} X_1X_2|\psi\rangle &= |\psi\rangle \\ Z_1Z_2|\psi\rangle &= |\psi\rangle \end{aligned}\right\}$$ $|\psi\rangle$ is stabilized by X_1X_2 and Z_1Z_2.

Pauli group G_n

Example: G_1

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

where I is the 2×2 unit matrix, and X, Y and Z are the Pauli matrices.

The Pauli group G_n on n qubits is the group generated by the operators described above applied to each of n qubits in the tensor product Hilbert space $(\mathbb{C}^2)^{\otimes n}$.

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. Then V_S is a vector space stabilized by S, and S is said to be the stabilizer of the space V_S.

Example: Consider $n = 3$ qubits and $S = \{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$:
The subspace stabilized by

$$Z_1Z_2 \text{ is spanned by } \{|000\rangle, |001\rangle, |110\rangle, |111\rangle\}$$
$$Z_2Z_3 \text{ is spanned by } \{|000\rangle, |100\rangle, |011\rangle, |111\rangle\}$$
$$Z_1Z_3 \text{ is spanned by } \{|000\rangle, |010\rangle, |101\rangle, |111\rangle\}$$

The elements $|000\rangle$ and $|111\rangle$ are fixed by all the operators from the set S, so V_s is spanned by these states.

We can work with only two operators, for example Z_1Z_2 and Z_2Z_3, because $Z_1Z_3 = (Z_1Z_2)(Z_2Z_3)$ and $(Z_1Z_2)^2 = I$. We now only need to show that the states are stabilized by the generators: $S = \{Z_1Z_2, Z_2Z_3\}$.

Conditions for a subgroup $S \subset G_n$ to be used as the stabilizer for a nontrivial V_s:
(i) the elements of S commute, and
(ii) the operator $-I$ is not an element of S.

Error correction using stabilizer codes

Suppose that $C(S)$ is a stabilizer code corrupted by an error $E \in G_n$:

1. 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.

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

3. The problem emerges if E commutes with all elements of S but $E \notin S$, that is $Eg = gE$ for all $g \in S$.

Centralizer Z_S:
the set $E \in G_n$ such that $Eg = gE$ for all $g \in S$.

Normalizer N_S:
the set $E \in G_n$ such that $EgE^\dagger \in S$.

For any subgroup $S \subset G_n$ not containing $-I$, $N(S) = Z(S)$.

Theorem
Let S be the stabilizer for a stabilizer code $C(S)$. Suppose $\{E_i\}$ is a set of operators in G_n such that $E_i^\dagger E_j \notin N(S) - S$ for all i and j. Then $\{E_i\}$ is a set of correctable errors for the code $C(S)$.

Three qubit bit flip code
is spanned by $|000\rangle$ and $|111\rangle$ with the stabilizer generated by $S = \{Z_1Z_2, Z_2Z_3\}$.

It can be shown explicitly that every possible product of two elements of the error set $\{I, X_1, X_2, X_3\}$ anticommutes with at least one element of the stabilizer, except for I which is an element of the stabilizer. 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 out by measuring the stabilizer generators. For example, if the error X_1 occured, the stabilizer is transformed into $\{-Z_1Z_2, Z_2Z_3\}$, so error syndrome measurement gives the results -1 and $+1$. Similarly the error X_2 gives the result -1 and -1, and X_3 gives the result $+1$ and -1.

The original state is recovered by applying the inverse of the error operator indicated by the error syndrome.

Shor nine qubit code

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

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

Stabilizer generators:

$$\begin{array}{c|ccccccccc}
g_1 & Z & Z & I & I & I & I & I & I & I \\
g_2 & I & Z & Z & I & I & I & I & I & I \\
g_3 & I & I & I & Z & Z & I & I & I & I \\
g_4 & I & I & I & I & Z & Z & I & I & I \\
g_5 & I & I & I & I & I & I & Z & Z & I \\
g_6 & I & I & I & I & I & I & I & Z & Z \\
g_7 & X & X & X & X & X & X & I & I & I \\
g_8 & I & I & I & X & X & X & X & X & X
\end{array}$$

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 $N(S)$. All other products of two errors from the error set of all single qubit errors for this code anticommutes with at least one element of the stabilizer S and thus are not in $N(S)$.

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

The encoded phase flip Z_L and bit flip X_L operations over the Shor code are realized by the operators

$$Z_L = X_1X_2X_3X_4X_5X_6X_7X_8X_9 \quad \text{and} \quad X_L = Z_1Z_2Z_3Z_4Z_5Z_6Z_7Z_8Z_9.$$

Steane $[7,1]$ code

$$\begin{aligned} |0_L\rangle &= \frac{1}{\sqrt{2^3}}(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ &\quad + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle) \\ |1_L\rangle &= \frac{1}{\sqrt{2^3}}(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\ &\quad + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle) \end{aligned}$$

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

$$\left(\begin{array}{c|c} H(C_2^{\perp}) & 0 \\ 0 & H(C_1) \end{array}\right).$$

$$\left(\begin{array}{c|c} H(C_2^\perp) & 0 \\ 0 & H(C_1) \end{array} \right).$$

The rows of this matrix correspond to stabilizer generators $g_1, \ldots, g_l$. The left side of the matrix contains "1" to indicate which generators contain Xs, and the right side contains "1" to indicate which generators contain Zs. In general case, the presence of "1" on both sides indicates Ys.

For the Stean code, with $C_1 = C$ and $C_2 = C^\perp$, we get

$$\left(\begin{array}{ccccccc|ccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array} \right).$$

Stabilizer generators for the Steane code

$$\begin{array}{c|ccccccc}
g_1 & I & I & I & X & X & X & X \\
g_2 & I & X & X & I & I & X & X \\
g_3 & X & I & X & I & X & I & X \\
g_4 & I & I & I & Z & Z & Z & Z \\
g_5 & I & Z & Z & I & I & Z & Z \\
g_6 & Z & I & Z & I & Z & I & Z
\end{array}$$

It can be shown that all single qubit errors form a correctable set for this code which implies that the Steane code can be used to correct an arbitrary single qubit error.

The encoded single qubit operations are

$$Z_L = Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7 \quad \text{and} \quad X_L = X_1 X_2 X_3 X_4 X_5 X_6 X_7.$$

Fault-tolerant quantum computation

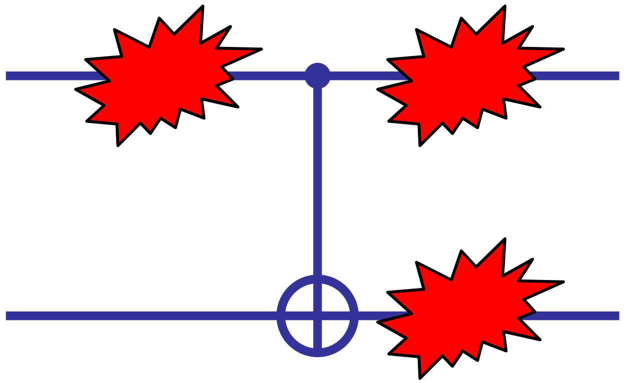
Reliable quantum computation can be achieved even with faulty gates provided the error probability per gate is below certain threshold.

To perform quantum computation on encoded quantum states, we replace an original quantum circuit by an encoded circuit, that is, each qubit by an encoded qubit, using for example Steane quantum error correcting code, and each operation by an appropriate encoded operation.

However, this is **not** sufficient for fault-tolerance.

Problems:

1. encoded gates can cause errors to propagate, and
2. encoded two-qubit operations, such as $CNOT$, can cause that an error on encoded control qubit spreads to the target qubit.



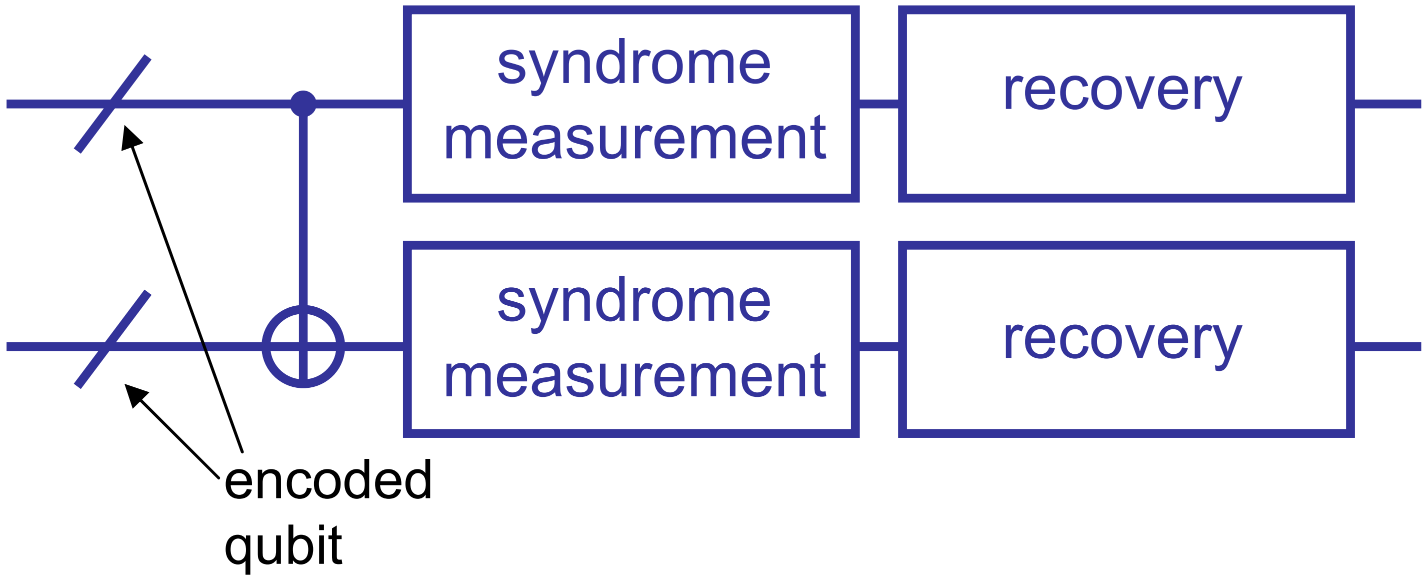
Fault-tolerant quantum operations are those which ensure that a failure anywhere during the computation can only propagate to a small number of qubits in each block of encoded data, so the error correction can effectively remove the error.

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 the threshold theorem

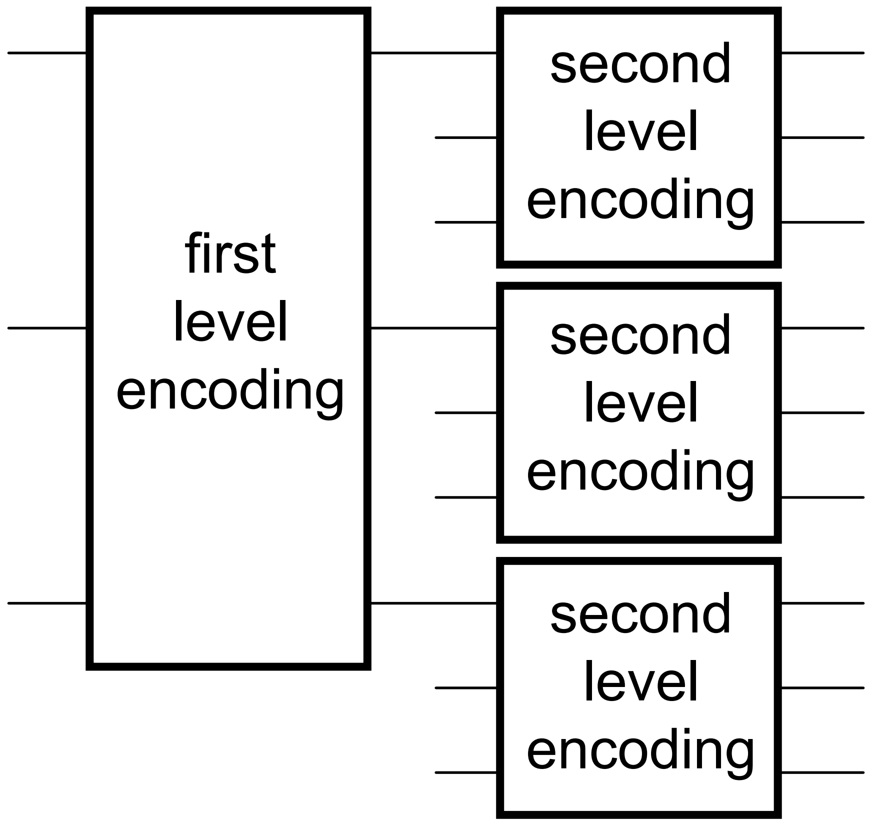
A fault-tolerant $CNOT$ gate:

The probability that this circuit introduces two or more errors in the first encoded block behaves as $O(p^2)$ where p is the probability of failure of individual components in the circuit.



Concatenated error correcting codes

Example: 9 qubit Shore code for correcting an arbitrary single qubit error



Threshold theorem

A quantum circuit containing $p(n)$ gates may be simulated with the probability of error at most ϵ using

$$O(poly(log p(n)/\epsilon)p(n))$$

gates on hardware whose components fail with the 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 $p_{th} \approx 10^{-4} - 10^{-5}$.

Physical realization: DiVincenzo criteria

Quantum computing

1. A scalable 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 coherence 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 realization of quantum computation

Quantum computing roadmap (2004) http://qist.lanl.gov

QC Approach	The DiVincenzo Criteria						
	Quantum Computation					QC Networkability	
	#1	#2	#3	#4	#5	#6	#7
NMR	red	yellow	yellow	green	yellow	red	red
Trapped Ion	yellow	green	yellow	green	green	yellow	yellow
Neutral Atom	yellow	green	yellow	yellow	yellow	yellow	yellow
Cavity QED	yellow	green	yellow	yellow	green	yellow	yellow
Optical	yellow	yellow	green	yellow	yellow	yellow	green
Solid State	yellow	yellow	yellow	yellow	yellow	red	red
Superconducting	yellow	green	yellow	yellow	yellow	red	red
Unique Qubits	This field is so diverse that it is not feasible to label the criteria with "Promise" symbols.						

Legend: green = a potentially viable approach has achieved sufficient proof of principle

yellow = a potentially viable approach has been proposed, but there has not been sufficient proof of principle

red = no viable approach is known

Noisy Intermediate Scale Quantum computers

NISQ constraints:

- limited number of qubits;

- limited connectivity between qubits;

- restricted (hardware specific) gate alphabets;

- limited circuit depth due to noise.