Quantum Information Processing: from Theory to Practice

Lecture 8: Quantum Error Correction

Outline

- From Classical to Quantum Error Correction (QEC)
  - Digitization of Quantum Errors
  - The Challenges of QEC
- Stabilizer Measurements
  - The Repetition QEC code
- Stabilizer Codes
  - QEC with Stabilizer Codes
  - The Shor Code
- Practical Considerations for QEC

Section 1

From Classical to Quantum Error Correction

Introduction

- Quantum computer works by controlling and manipulating qubits
- There is currently no preferred qubit technology
  - photons
  - trapped ions
  - superconducting circuits
  - spins in semiconductors
- For all technologies, it is difficult to isolate the qubits from the external noise. Quantum computation errors are inevitable
- Need for some active error correction
- There is a well-developed theory of error correction that works for classical bits. However, adapting classical methods to QEC is not straightforward due to:
  - No-cloning Theorem
  - Collapse of the qubit state after measurement

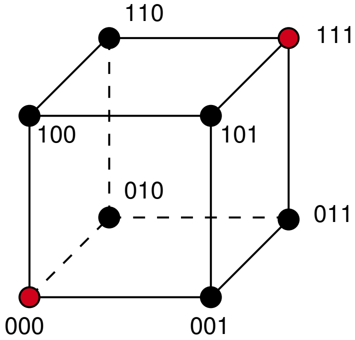
Classical Error Correction

- Assume information is encoded as a sequence of bits '0' and '1'
- The information sequence can be protected from errors by adding some redundant bits to the sequence
- The redundancy is added according to some precise rules known as an error correcting code

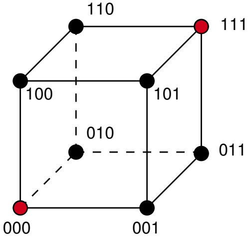
Example: 3-bit Repetition code. One bit of information is repeated 3 times.

$$0 \mapsto 000, \quad 1 \mapsto 111$$

The strings 000 and 111 are called codewords.



Classical Correction of a Bit-Flip



- Suppose Alice sends the 3-bit message 000 to Bob
  - If there is a single bit-flip error during transmission, Bob receives, for example, 010. Through a majority vote, Bob can infer that the intended message was the logical '0'
  - If the codeword is subject to 2 bit-flip errors, the majority vote will always lead to the incorrect codeword
  - If there are 3 bit-flip errors, Bob receives the codeword 111: He believes that no error has occurred.
- In general, let d be the minimum number of bit errors that will change one codeword to another (i.e., the distance of the code). Then,

$$d = 2t + 1$$

  where t is the number of bit flips that can be corrected
- Classical error correcting codes are denoted with the triple (n, k, d), where n is the length of the codewords and k is the number of encoded bits

The Digitization of Quantum Errors

- The general qubit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle\,, \qquad |\alpha|^2 + |\beta|^2 = 1,$$

  can assume a continuum of values between its basis states

- It seems that the qubit can be subject to an infinite number of errors (for example, any unitary U that acts on $|\psi\rangle$)
- However, we know that any 2×2 unitary matrix can be expressed in terms of the Pauli basis $\{I, X, Y, Z\}$:

$$\begin{aligned} U|\psi\rangle &= \alpha_I I|\psi\rangle + \alpha_X X|\psi\rangle + \alpha_Z Z|\psi\rangle + \alpha_Y Y|\psi\rangle \\ (Y = iXZ) &= \alpha_I I|\psi\rangle + \alpha_X X|\psi\rangle + \alpha_Z Z|\psi\rangle + \alpha_Y iXZ|\psi\rangle \end{aligned}$$

- A quantum error correcting code with the ability to correct errors described by the X and the Z Pauli matrices will be able to correct any error U

Quantum Errors Types

There are two fundamental quantum error types:

- Pauli X-type errors are the quantum analogue of classical bit-flips

$$X|0\rangle = |1\rangle\,, \qquad X|1\rangle = |0\rangle\,, \qquad X|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$$

- Pauli Z-type errors have no classical analogue. They are often referred to as phase-flips

$$Z|0\rangle = |0\rangle\,, \qquad Z|1\rangle = -|1\rangle\,, \qquad Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$$

The Challenges of Quantum Error Correction

There are a number of complications for a straightforward application of classical error correcting codes to the quantum world:

- No-cloning theorem: contrary to classical codes, where redundant bits can be added to the sequences in an arbitrary manner, we cannot perform the operation

  $$U_{\text{clone}}(|\psi\rangle \times |0\rangle) = (|\psi\rangle \times |\psi\rangle)$$

  for any qubit state $|\psi\rangle$
- A new type of error: quantum error correcting codes must be designed to tackle also phase-flip errors, which are not present in classical systems
- State collapse: in classical systems, data sequences can be read without compromising the encoded information. In quantum systems, however, any measurement performed as part of the error correction must be chosen so as not to cause the state to collapse and erase the encoded information

Section 2

Stabilizer Measurements

How to Create Redundancy

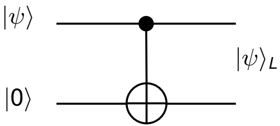
We will show how to add redundancy by means of an example: The two-qubit repetition code, which can detect up to a single bit-flip error.

Encoding: We map the qubit $|\psi\rangle$ into a 4-dimensional Hilbert space as follows:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \longrightarrow |\psi\rangle_L = \alpha\,|00\rangle + \beta\,|11\rangle = \alpha\,|0\rangle_L + \beta\,|1\rangle_L$$

where the logical codewords are $|0\rangle_L = |00\rangle$ and $|1\rangle_L = |11\rangle$.

Circuit Diagram: We can encode by simply using a CNOT gate



Note that $|\psi\rangle_L = \alpha\,|00\rangle + \beta\,|11\rangle \neq |\psi\rangle \otimes |\psi\rangle$, i.e., we did not clone the state. However, $|\psi\rangle_L$ is an entangled state.

The Code and the Error Subspaces

After encoding, the logical qubit is in a subspace $\mathcal{C}$ of the 4-dimensional Hilbert space $\mathcal{H}_4 = \text{span}\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$:

$$|\psi\rangle_L \in \mathcal{C} = \text{span}\{|00\rangle, |11\rangle\} \subset \mathcal{H}_4$$

$\mathcal{C}$ is called codespace

If $|\psi\rangle_L$ is subject to a bit-flip error on the first qubit, then the resulting state is

$$X_1 |\psi\rangle_L = \alpha |10\rangle + \beta |01\rangle \in \mathcal{F} \subset \mathcal{H}_4$$

$\mathcal{F}$ is called error subspace.

Note that $\mathcal{C} \perp \mathcal{F}$, hence we can determine to which subspace the logical qubit belongs to via a projective measurement without compromising the encoded quantum information. Measurements of this type are called stabilizer measurements.

Stabilizer Measurements

- Consider the unitary Z_1Z_2 applied to the logical state $|\psi\rangle_L$:

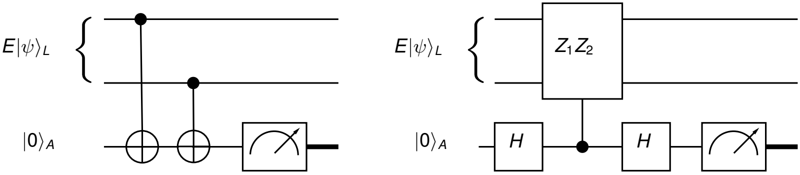
$$Z_1Z_2\,|\psi\rangle_L = Z_1Z_2(\alpha\,|00\rangle + \beta\,|11\rangle) = (+1)\,|\psi\rangle_L \in \mathcal{C}$$

- The Z_1Z_2 operator is said to stabilize the logical qubit $|\psi\rangle_L$ as it leaves it unchanged.
- Conversely,

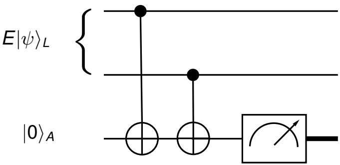
$$Z_1Z_2(X_1\,|\psi\rangle_L) = -X_1Z_1Z_2\,|\psi\rangle_L = -X_1\,|\psi\rangle_L \in \mathcal{F}$$

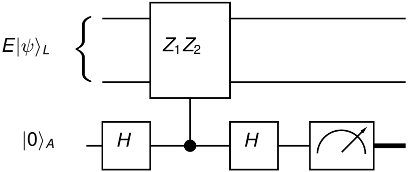
- For either outcome, the information encoded in the α and β coefficients of the logical state remains undisturbed.

Circuit Diagram: Two possible implementations are as follows



Measurement Outcome





- The outcome of the measurement of the ancilla qubit is referred to as a syndrome, and tells us whether or not the logical state has been subject to an error.
- The table shows the measured syndromes for all bit-flip error types in the two-qubit code

Error E	Syndrome
$I_1 I_2$	0
$X_1 I_2$	1
$I_1 X_2$	1
$X_1 X_2$	0

- Note that this code is not able to detect a double error X_1X_2. However, if the errors on physical qubits occur independently and with the same probability p_X, then a double error occurs with probability p_X^2
- If p_X is sufficiently small, then for a single qubit $|\psi\rangle$ without QEC the prob. of error is p_X, while for the logical qubit $|\psi\rangle_L$ the prob. of error is $\approx p_X^2 \ll p_X$

The 3-qubit Error Correction Code

Error E	Syndrome
$I_1 I_2$	0
$X_1 I_2$	1
$I_1 X_2$	1
$X_1 X_2$	0

- The syndrome of the 2-qubit error correction code does not provide enough information to infer which qubit the X error occurred on
- In order to be able to correct the error, multiple stabilizer measurements need to be performed
- Consider an entangled 3-party state

$$|\psi\rangle_L = \alpha |000\rangle + \beta |111\rangle$$

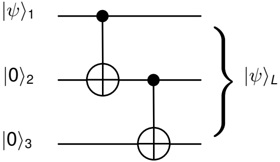
which occupies an 8-dimensional Hilbert space that can be partitioned as follows:

$$\mathcal{C} = \text{span}\{|000\rangle, |111\rangle\}, \qquad \mathcal{F}_1 = \text{span}\{|100\rangle, |011\rangle\},$$
$$\mathcal{F}_2 = \text{span}\{|010\rangle, |101\rangle\}, \qquad \mathcal{F}_3 = \text{span}\{|001\rangle, |110\rangle\},$$

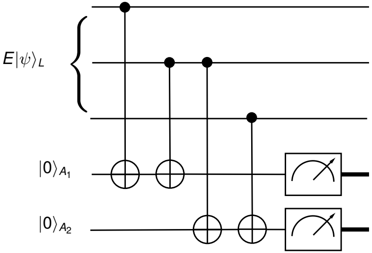
where $\mathcal{C}$ is the logical space and $\mathcal{F}_{1,2,3}$ are the logical error spaces such that $X_i |\psi\rangle_L \in \mathcal{F}_i$, for $i = 1, 2, 3$.

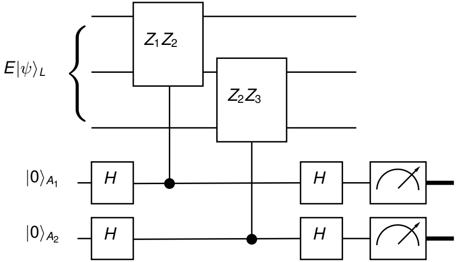
The 3-qubit Error Correction Code: Encoding and Syndrome Extraction

Encoding Circuit:



Syndrome Extraction Circuits:





The 3-qubit Error Correction Code: Syndrome Table

Error E	Syndrome	Error E	Syndrome
$I_1 I_2 I_3$	00	$X_1 X_2 X_3$	00
$X_1 I_2 I_3$	10	$I_1 X_2 X_3$	10
$I_1 X_2 I_3$	11	$X_1 I_2 X_3$	11
$I_1 I_2 X_3$	01	$X_1 X_2 I_3$	01

- Each single-qubit error produces a unique 2-bit syndrome $S = s_1 s_2$, enabling us to choose a suitable recovery operation
- We can use the 3-qubit repetition code in two alternative ways:
  - to detect up to 2-qubit errors (the error $E = X_1 X_2 X_3$ is undetectable)
  - to correct up to one-qubit error (the errors $E = \{X_1 X_2 X_3, I_1 X_2 X_3, X_1 I_2 X_3, X_1 X_2 I_3\}$ are uncorrectable
- If qubits were only susceptible to X-errors, the 3-qubit repetition code would have a distance of $d = 3$
- However, there are also phase-flip errors Z. Consider the same codespace $\mathcal{C}$ with logical states

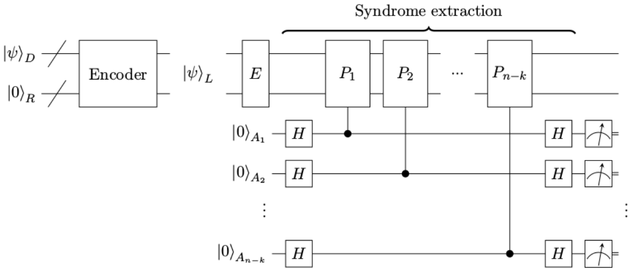
$$|+\rangle_L = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \qquad |-\rangle_L = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle).$$

Since $Z_1 |+\rangle_L = |-\rangle_L$, the code is unable to detect a single-qubit Z-error. Hence, the 3-qubit repetition code has a quantum distance $d = 1$.

Section 3

Stabilizer Codes

Generalization to an [[n, k, d]] Stabilizer Code



- A quantum data register $|\psi\rangle_D = |\psi_1\psi_2 \ldots \psi_k\rangle$ is entangled with redundancy bits $|0\rangle_R = |0_1 0_2 \ldots 0_{n-k}\rangle$ to create a logical qubit $|\psi\rangle_L$
- After encoding, a sequence of $n - k$ stabilizer checks P_i are performed on the register, and each result copied to an ancilla qubit A_i
- The subsequent measurement of the ancilla qubits provides an $(n - k)$-bit syndrome

Properties of the Stabilizers

- P_i is a tensor product of n matrices from the Pauli group

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

  Example: $P_i = I \otimes X \otimes I \otimes Y$ is an element of the 4-qubit Pauli group.

- P_i must stabilize all logical states $|\psi\rangle_L$ of the code, i.e.,

$$P_i |\psi\rangle_L = (+1) |\psi\rangle_L, \qquad \forall |\psi\rangle_L$$

- All stabilizers must commute with one another:

$$P_i P_j = P_j P_i, \qquad \forall i, j$$

  so that the stabilizers can be measured independently of their ordering.

Remarks:

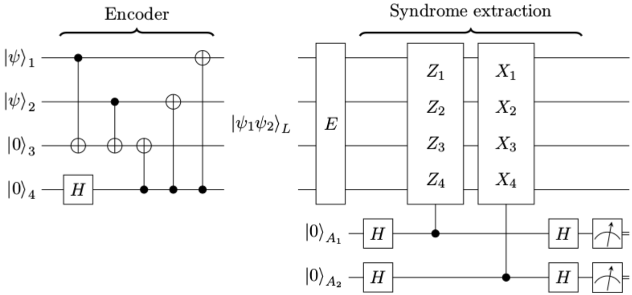
- Note that $P_i P_j$ is also a stabilizer: $P_i P_j |\psi\rangle_L = P_i(+1) |\psi\rangle_L = (+1) |\psi\rangle_L$
- Let $\mathcal{S} = \{P_i\}$ be the set of stabilizers. It is useful to find a minimal set of stabilizers $\mathcal{S} = \langle G_1, G_2, \ldots, G_{n-k}\rangle$ where each stabilizer G_i cannot be seen as a product of any of the other elements $G_j \in \mathcal{S}$.

Example: The [[4, 2, 2]] Detection Code

- The [[4, 2, 2]] detection code is the smallest stabilizer code able to detect both X- and Z-errors

$$\mathcal{C}_{[[4,2,2]]} = \text{span}\left\{ \begin{array}{l} |00\rangle_L = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle) \\ |01\rangle_L = \frac{1}{\sqrt{2}}(|0110\rangle + |1001\rangle) \\ |10\rangle_L = \frac{1}{\sqrt{2}}(|1010\rangle + |0101\rangle) \\ |11\rangle_L = \frac{1}{\sqrt{2}}(|1100\rangle + |0011\rangle) \end{array} \right\}$$

$$\mathcal{S}_{[[4,2,2]]} = \langle X_1X_2X_3X_4, Z_1Z_2Z_3Z_4 \rangle$$



Example: The [[4, 2, 2]] Detection Code

- Consider a single-qubit error $E = \{X_1, X_2, X_3, X_4\}$. Then

$$Z_1 Z_2 Z_3 Z_4 E \left|\psi\right\rangle_L = Z_1 Z_2 Z_3 Z_4 X_i \left|\psi\right\rangle_L = -X_i Z_1 Z_2 Z_3 Z_4 \left|\psi\right\rangle_L = -X_i \left|\psi\right\rangle_L$$

  will trigger a non-zero syndrome
- Consider a single-qubit error $E = \{Z_1, Z_2, Z_3, Z_4\}$. Then

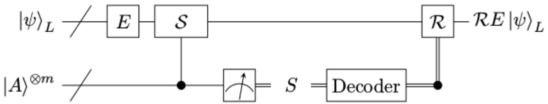
$$X_1 X_2 X_3 X_4 E \left|\psi\right\rangle_L = X_1 X_2 X_3 X_4 Z_i \left|\psi\right\rangle_L = -Z_i X_1 X_2 X_3 X_4 \left|\psi\right\rangle_L = -Z_i \left|\psi\right\rangle_L$$

  will trigger a non-zero syndrome

Error E	Syndrome	Error E	Syndrome	Error E	Syndrome
X_1	10	Z_1	01	Y_1	11
X_2	10	Z_2	01	Y_2	11
X_3	10	Z_3	01	Y_3	11
X_4	10	Z_4	01	Y_4	11

- We can detect the type of error, but not the position of the error, i.e., we cannot correct the error
- The distance of the code is $d = 2$

Quantum Error Correction with Stabilizer Codes



- If the distance of the code is $d = 2t + 1$, the number of correctable errors is t
- If $t \geq 1$ (hence $d \geq 3$), then we can try to correct the error
- A generating set of stabilizers $\mathcal{S}$ is measured on the logical state to yield an $(n-k)$-bit syndrome S
- The syndrome is processed by a decoder to determine the best operation $\mathcal{R}$ such that $\mathcal{R}E\,|\psi\rangle_L \in \mathcal{C}_{[[n,k,d]]}$
- The decoding is successful if $\mathcal{R}E\,|\psi\rangle_L = (+1)\,|\psi\rangle_L$. A possible solution is when $\mathcal{R}E = P \in \mathcal{S}$ is a code stabilizer.

Example: The [[9, 1, 3]] Shor Code

- The [[9, 1, 3]] Shor code was the first QEC scheme to be proposed
- It is obtained by concatenation of the 3-qubit repetition code for bit-flips

$$\mathcal{C}_{3b} = \text{span}\left\{|0\rangle_{3b} = |000\rangle\,, |1\rangle_{3b} = |111\rangle\right\}, \quad \mathcal{S}_{3b} = \langle Z_1 Z_2, Z_2 Z_3\rangle$$

  and the 3-qubit repetition code for phase-flips

$$\mathcal{C}_{3p} = \text{span}\left\{|0\rangle_{3p} = |+++\rangle\,, |1\rangle_{3p} = |---\rangle\right\}, \quad \mathcal{S}_{3p} = \langle X_1 X_2, X_2 X_3\rangle$$

- Code concatenation is a technique where the output of one code is embedded in the input of another code. For the Shor code, the logical qubits are obtained with the following concatenations:

$$|0\rangle_{3p} = |+++\rangle \xrightarrow{\text{concatenation}} |0\rangle_9 = |+\rangle_{3b}|+\rangle_{3b}|+\rangle_{3b}\,, \qquad |+\rangle_{3b} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

$$|1\rangle_{3p} = |---\rangle \xrightarrow{\text{concatenation}} |1\rangle_9 = |-\rangle_{3b}|-\rangle_{3b}|-\rangle_{3b}\,, \qquad |-\rangle_{3b} = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$$

Example: The [[9, 1, 3]] Shor Code

- Rewriting the logical states in the computational basis, we get

$$\mathcal{C}_{[[9,1,3]]} = \text{span}\left\{ \begin{array}{l} |0\rangle_9 = \frac{1}{\sqrt{8}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \\ |1\rangle_9 = \frac{1}{\sqrt{8}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle) \end{array} \right\}$$

$$\mathcal{S}_{[[9,1,3]]} = \langle Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9, \\ X_1X_2X_3X_4X_5X_6, X_4X_5X_6X_7X_8X_9\rangle$$

- The first six terms are the stabilizers of the bit-flip codes in the 3 blocks of the code
- The final two stabilizers derive from the stabilizers of the phase-flip code

Example: The $[[9,1,3]]$ Shor Code

Error E	Syndrome	Recovery $\mathcal{R}$	Error E	Syndrome	Recovery $\mathcal{R}$
X_1	10000000	X_1	Z_1	00000010	Z_1
X_2	11000000	X_2	Z_2	00000010	Z_1
X_3	01000000	X_3	Z_3	00000010	Z_1
X_4	00100000	X_4	Z_4	00000011	Z_4
X_5	00110000	X_5	Z_5	00000011	Z_4
X_6	00010000	X_6	Z_6	00000011	Z_4
X_7	00001000	X_7	Z_7	00000001	Z_7
X_8	00001100	X_8	Z_8	00000001	Z_7
X_9	00000100	X_9	Z_9	00000001	Z_7

- Each of the X-errors produce unique syndromes: all single-qubit X-errors can be corrected with $\mathcal{R}_i = X_i$
- Z-errors that occur in the same block of the code have the same syndrome. However, this fact does not reduce the code distance:
  - Suppose $E = Z_1$. Then the recovery is $\mathcal{R}E\,|\psi\rangle_9 = Z_1 Z_1\,|\psi\rangle_9 = |\psi\rangle_9$
  - Suppose $E = Z_2$. Then the recovery is $\mathcal{R}E\,|\psi\rangle_9 = Z_1 Z_2\,|\psi\rangle_9 = |\psi\rangle_9$, because $Z_1 Z_2 \in \mathcal{S}$ is a stabilizer of the code
- Shor's 9-qubit code can correct all single-qubit errors and has distance $d = 3$

Section 4

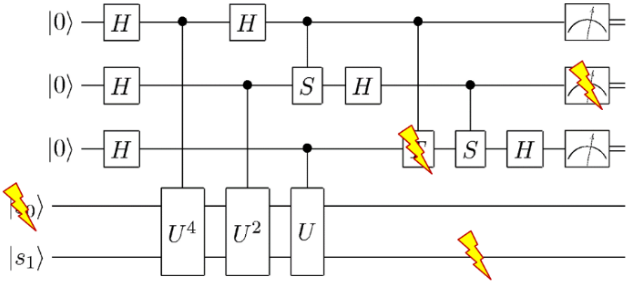
Practical Considerations for QEC

Efficient Decoding Algorithms

- Given a code syndrome S, the decoder has to find the best recovery $\mathcal{R}$
- There are 2^{n-k} possible syndromes:
  - For small redundancy $n-k$, it is possible to precompute look-up tables that list the best recovery $\mathcal{R}$ for each syndrome
  - For large redundancy, approximate inference techniques can be used to determine the most likely error that occurred
- There is no known universal decoding algorithm that can be efficiently applied to all QEC codes
- Ad-hoc decoding algorithms are designed for specific code constructions:
  - graph-based decoding (belief propagation, minimum-weight perfect matching)
  - machine learning approaches

Fault Tolerance

- So far, we have assumed that errors only occur in certain locations in the circuit (for example, where the unitary E is located)
- Thus, we are implicitly assuming that all encoding and syndrome extraction apparatus operates without error. However, two-qubit gates as well as measurement operations can be dominant sources of error.
- A QEC code is fault tolerant if it can account for at most t errors that occur at any location in the circuit
- Fault tolerant QEC codes can be obtained by
  - adding more redundancy compared to the original code
  - perform two or more rounds of stabilizer measurements and compare syndromes over time



Fault Tolerance

- Errors are generated and start to accumulate very quickly
- The only way to protect quantum information is to constantly correct the newly occurring errors and be fast enough so that not too many errors accumulate, which would end up creating uncorrectable logical errors