Quantum Error Correction: A Tutorial

Navin Kashyap

Department of Electrical Communication Engineering
Indian Institute of Science

Outline

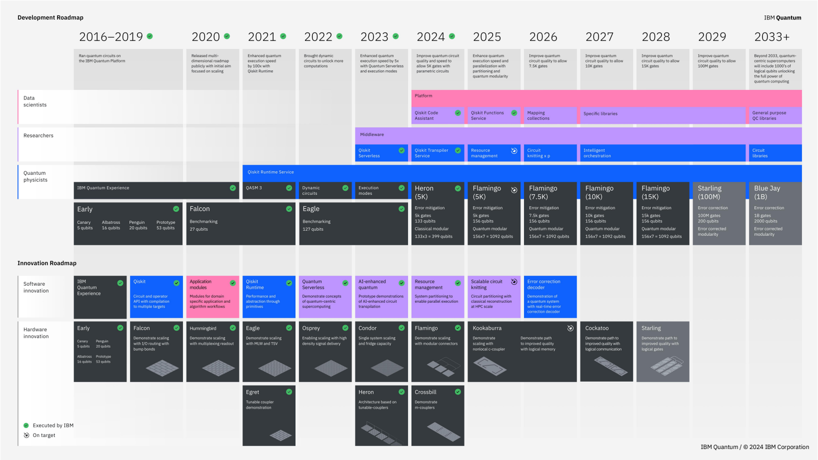
Background and Motivation

NISQ-Era and Beyond

John Preskill, *Quantum Computing in the NISQ era and beyond*, Quantum, vol. 2, p. 79, 2018. [Online] arXiv:1801.00862v3

- Noisy Intermediate-Scale Quantum (NISQ) technology
  - up to a few hundred qubits
  - faulty gates
- 5-10 year horizon
  - thousands of qubits and beyond
  - fault-tolerant, based on quantum error correction.

The IBM Quantum Computing Roadmap



Quantum Computing Technologies

Various quantum computing technologies are in development:

- Superconducting qubits — IBM, Google, IQM, Rigetti etc.
- Photonics / bosonic computing — Xanadu, ORCA Computing, PsiQuantum etc.
- Trapped ions — IonQ, Oxford Ionics, Quantinuum etc.
- Neutral atoms — Pasqal, QuEra, planqc etc.

Many other efforts at universities and start-ups around the world.

Quantum Error Correction Basics

Logical and Physical Qubits

- A qubit is the state of a two-state quantum system. Formally, it is a quantum state living in a 2-dimensional state space, $\mathcal{H}$:

$$|\psi\rangle \;=\; \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \text{where } \alpha, \beta \in \mathbb{C}, \text{ with } |\alpha|^2 + |\beta^2| = 1.$$

Logical and Physical Qubits

- A qubit is the state of a two-state quantum system. Formally, it is a quantum state living in a 2-dimensional state space, $\mathcal{H}$:

  $$|\psi\rangle \ = \ \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \text{where } \alpha, \beta \in \mathbb{C}, \text{ with } |\alpha|^2 + |\beta^2| = 1.$$

- Physical Qubits. These are the physical objects that behave as two-state quantum systems.

  Physical qubits are highly error-prone due to decoherence, i.e., loss of information to the environment.

- Logical Qubits. These are the abstract qubits upon which a quantum algorithm is executed.

Logical and Physical Qubits

- A qubit is the state of a two-state quantum system. Formally, it is a quantum state living in a 2-dimensional state space, $\mathcal{H}$:

  $$|\psi\rangle \;=\; \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \text{where } \alpha, \beta \in \mathbb{C}, \text{ with } |\alpha|^2 + |\beta^2| = 1.$$

- Physical Qubits. These are the physical objects that behave as two-state quantum systems.

  Physical qubits are highly error-prone due to decoherence, i.e., loss of information to the environment.

- Logical Qubits. These are the abstract qubits upon which a quantum algorithm is executed.

- Dozens of physical qubits are typically required to sustain a single logical qubit for the purposes of computation.

Bit-Flip and Phase-Flip Errors

- A bit-flip error on a physical qubit is an X gate acting on that qubit: $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

$$X|0\rangle = |1\rangle \quad \text{and} \quad X|1\rangle = |0\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \ \text{---}\boxed{X}\text{---} \ \alpha|1\rangle + \beta|0\rangle$$

Bit-Flip and Phase-Flip Errors

- A bit-flip error on a physical qubit is an X gate acting on that qubit: $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

$$X|0\rangle = |1\rangle \quad \text{and} \quad X|1\rangle = |0\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \;\text{———}\boxed{X}\text{———}\; \alpha|1\rangle + \beta|0\rangle$$

- A phase-flip error on a physical qubit is a Z gate acting on that qubit: $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

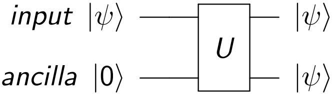
$$Z|0\rangle = |0\rangle \quad \text{and} \quad Z|1\rangle = -|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \;\text{———}\boxed{Z}\text{———}\; \alpha|0\rangle - \beta|1\rangle$$

The No-Cloning Theorem

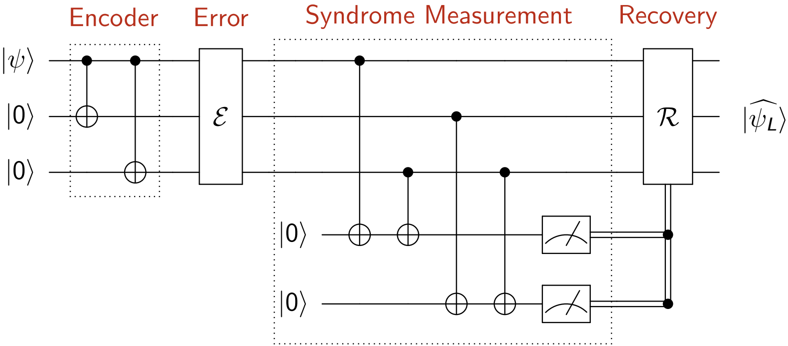
Theorem

There is no unitary gate U that operates as shown:



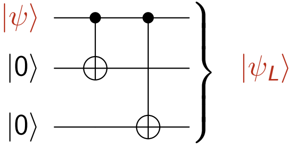
In other words, there is no quantum gate that can create an exact replica of an input qubit in an arbitrary (unknown) state.

The 3-Qubit Single-Bit-Flip-Correcting Code



- One logical qubit is encoded within three physical qubits
- Can correct a bit-flip (X) error in at most one of the three physical qubits

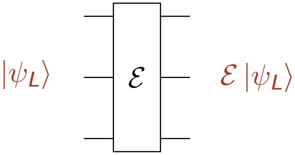
Encoder



$$
\begin{aligned}
|0\rangle &\longmapsto |000\rangle =: |0_L\rangle \\
|1\rangle &\longmapsto |111\rangle =: |1_L\rangle
\end{aligned}
$$

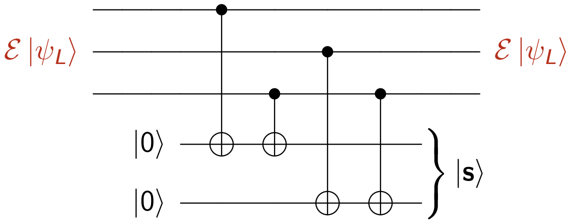
$$
\underbrace{\alpha\,|0\rangle + \beta\,|1\rangle}_{|\psi\rangle} \longmapsto \underbrace{\alpha\,|000\rangle + \beta\,|111\rangle}_{|\psi_L\rangle}
$$

Error



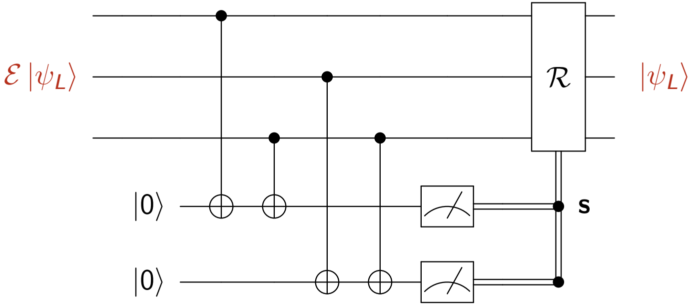
$\mathcal{E}$	$\mathcal{E}\,\vert\psi_L\rangle$	description
$I \otimes I \otimes I$	$\alpha\,\vert 000\rangle + \beta\,\vert 111\rangle$	no error
$X \otimes I \otimes I$	$\alpha\,\vert 100\rangle + \beta\,\vert 011\rangle$	bit-flip on 1st qubit
$I \otimes X \otimes I$	$\alpha\,\vert 010\rangle + \beta\,\vert 101\rangle$	bit-flip on 2nd qubit
$I \otimes I \otimes X$	$\alpha\,\vert 001\rangle + \beta\,\vert 110\rangle$	bit-flip on 3rd qubit

Syndrome Qubits



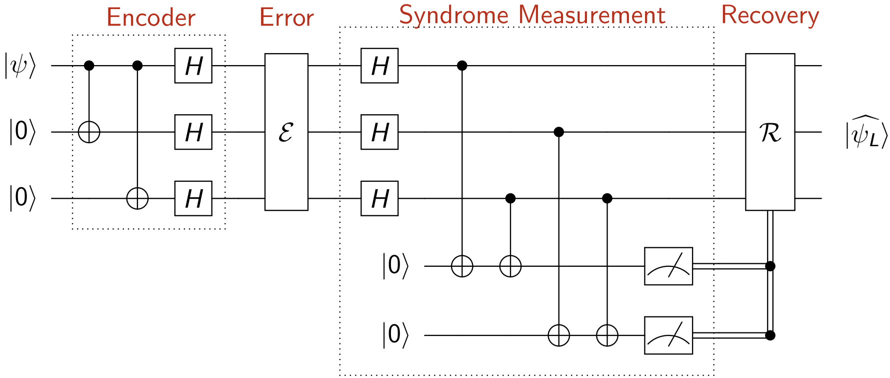
$\mathcal{E}$	$\mathcal{E}\,\vert\psi_L\rangle$	Syndrome $\vert\mathbf{s}\rangle$
$I \otimes I \otimes I$	$\alpha\,\vert 000\rangle + \beta\,\vert 111\rangle$	$\vert 00\rangle$
$X \otimes I \otimes I$	$\alpha\,\vert 100\rangle + \beta\,\vert 011\rangle$	$\vert 10\rangle$
$I \otimes X \otimes I$	$\alpha\,\vert 010\rangle + \beta\,\vert 101\rangle$	$\vert 01\rangle$
$I \otimes I \otimes X$	$\alpha\,\vert 001\rangle + \beta\,\vert 110\rangle$	$\vert 11\rangle$

Syndrome Measurement and Recovery



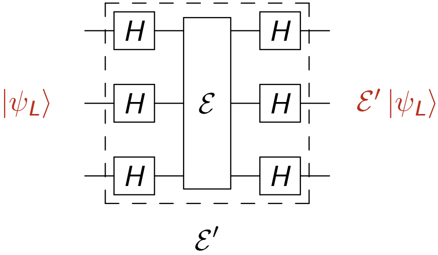
$\mathcal{E}$	$\mathcal{E}\,\|\psi_L\rangle$	s	$\mathcal{R}$
$I \otimes I \otimes I$	$\alpha\,\|000\rangle + \beta\,\|111\rangle$	00	$I \otimes I \otimes I$
$X \otimes I \otimes I$	$\alpha\,\|100\rangle + \beta\,\|011\rangle$	10	$X \otimes I \otimes I$
$I \otimes X \otimes I$	$\alpha\,\|010\rangle + \beta\,\|101\rangle$	01	$I \otimes X \otimes I$
$I \otimes I \otimes X$	$\alpha\,\|001\rangle + \beta\,\|110\rangle$	11	$I \otimes I \otimes X$

The 3-Qubit Single-Phase-Flip-Correcting Code



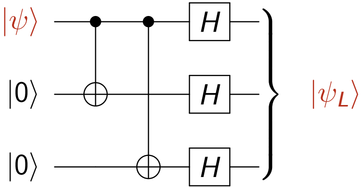
- One logical qubit is encoded within three physical qubits
- Can correct a phase-flip (Z) error in at most one of the three physical qubits

Converting Z-Errors to X-Errors



$\mathcal{E}$	$\mathcal{E}'$
$I \otimes I \otimes I$	$I \otimes I \otimes I$
$Z \otimes I \otimes I$	$X \otimes I \otimes I$
$I \otimes Z \otimes I$	$I \otimes X \otimes I$
$I \otimes I \otimes Z$	$I \otimes I \otimes X$

Encoder



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

$$
\underbrace{\alpha\,|0\rangle + \beta\,|1\rangle}_{|\psi\rangle} \longmapsto \underbrace{\alpha\,|+++\rangle \;+\; \beta\,|---\rangle}_{|\psi_L\rangle}
$$

Shor's Code

Shor (1995)

- Obtained by concatenating the 3-qubit phase-flip code with the 3-qubit bit-flip code.
- Outer code: 3-qubit phase-flip code

$$|0\rangle \longmapsto |+++\rangle \quad \text{and} \quad |1\rangle \longmapsto |---\rangle$$

- Inner code: 3-qubit bit-flip code — each $|+\rangle$ or $|-\rangle$ of the outer code is further encoded as

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \longmapsto \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \longmapsto \frac{|000\rangle - |111\rangle}{\sqrt{2}}$$

Shor's Code

Shor (1995)

- The resulting code encodes one logical qubit into $3 \times 3 = 9$ physical qubits:

$$|0\rangle \longmapsto |0_L\rangle := \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right)^{\otimes 3}$$

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

$$\underbrace{\alpha\,|0\rangle + \beta\,|1\rangle}_{|\psi\rangle} \longmapsto \underbrace{\alpha\,|0_L\rangle + \beta\,|1_L\rangle}_{|\psi_L\rangle}$$

Shor's Code

Shor (1995)

- The resulting code encodes one logical qubit into $3 \times 3 = 9$ physical qubits:

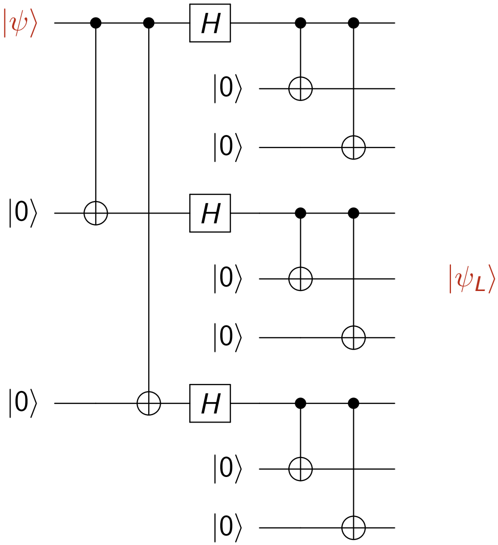
$$|0\rangle \longmapsto |0_L\rangle := \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right)^{\otimes 3}$$

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

$$\underbrace{\alpha\,|0\rangle + \beta\,|1\rangle}_{|\psi\rangle} \longmapsto \underbrace{\alpha\,|0_L\rangle + \beta\,|1_L\rangle}_{|\psi_L\rangle}$$

- This code is capable of correcting an *arbitrary* unitary error on any one of the 9 physical qubits.

Encoder



$|\psi\rangle$
$|0\rangle$
$|0\rangle$
H
H
H
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|\psi_L\rangle$

Bit-flip and Phase-flip Errors

- Encoded $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:

$$\alpha\left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right)$$

$$+\beta\left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right)$$

- Bit-flip error in 5th qubit:

$$\alpha\left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|010\rangle + |101\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right)$$

$$+\beta\left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|010\rangle - |101\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right)$$

Bit-flip and Phase-flip Errors

- Encoded $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:

$$\alpha\left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right)$$

$$+\beta\left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right)$$

- Bit-flip error in 5th qubit:

$$\alpha\left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|010\rangle + |101\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right)$$

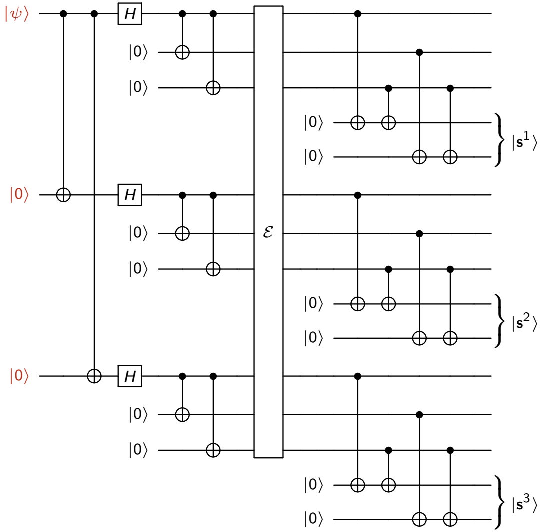
$$+\beta\left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|010\rangle - |101\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right)$$

- Phase-flip error in 7th qubit:

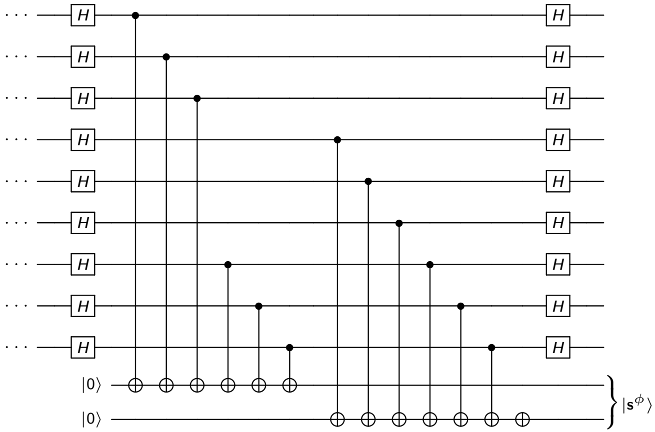
$$\alpha\left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right)$$

$$+\beta\left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right)$$

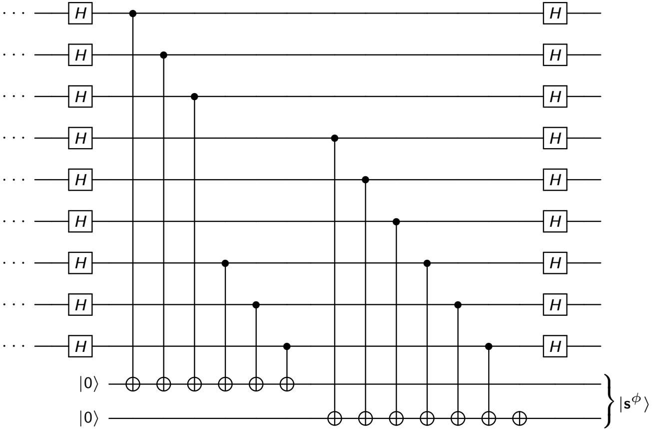
Syndrome Qubits for Bit-Flip Error Correction



Syndrome Qubits for Phase-Flip Error Correction



Syndrome Qubits for Phase-Flip Error Correction



- Thus, a total number of eight syndrome qubits are used:
  - 6 for bit-flip errors
  - 2 for phase-flip errors

Shor's Code: Error Correction

Shor's code is capable of correcting the following types of errors:

- a single bit-flip (X) error in each of the three blocks of 3 physical qubits
- a single phase-flip (Z) error affecting exactly one of the three blocks of 3 physical qubits
- an XZ-error, i.e., a bit-flip followed by a phase-flip on the same physical qubit

Shor's Code: Error Correction

Shor's code is capable of correcting the following types of errors:

- a single bit-flip (X) error in each of the three blocks of 3 physical qubits
- a single phase-flip (Z) error affecting exactly one of the three blocks of 3 physical qubits
- an XZ-error, i.e., a bit-flip followed by a phase-flip on the same physical qubit
- an *arbitrary* unitary error operator acting on any one of the 9 physical qubits!

Linear Algebra: An ON Basis of $\mathbb{C}^{2\times 2}$

- The matrices

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \; Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \; XZ = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

form an orthonormal basis of $\mathbb{C}^{2\times 2}$ with respect to the Hilbert-Schmidt inner product

$$(A, B) \; := \; \frac{1}{2}\,\mathrm{tr}(A^\dagger B)$$

Linear Algebra: An ON Basis of $\mathbb{C}^{2\times 2}$

- The matrices

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad XZ = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

  form an orthonormal basis of $\mathbb{C}^{2\times 2}$ with respect to the Hilbert-Schmidt inner product

$$(A, B) \;:=\; \frac{1}{2}\,\mathrm{tr}(A^\dagger B)$$

- Thus, any 2×2 complex matrix A is (uniquely) expressible as $\alpha_1 I_2 + \alpha_2 X + \alpha_3 Z + \alpha_4 (XZ)$ for some $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{C}$

- If A is unitary, then $|\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 + |\alpha_4|^2 \;=\; 1.$

Shor's Code: Error Correction

- Suppose that $|\psi_L\rangle = \alpha\,|0_L\rangle + \beta\,|1_L\rangle$ is affected by a single-qubit error operator

$$\mathcal{E} \;=\; I_2 \otimes \cdots \otimes I_2 \otimes U \otimes I_2 \otimes \cdots \otimes I_2,$$

  where U is an arbitrary 2×2 unitary operator acting on the ith qubit of $|\psi_L\rangle$.

- Write $U \;=\; \alpha_1 I_2 + \alpha_2 X + \alpha_3 Z + \alpha_4 (XZ)$, with $|\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 + |\alpha_4|^2 \;=\; 1$.

- Then,

$$\mathcal{E}\,|\psi_L\rangle \;=\; \alpha_1\,|\psi_L\rangle + \alpha_2\,X_i\,|\psi_L\rangle + \alpha_3\,Z_i\,|\psi_L\rangle + \alpha_4\,X_i Z_i\,|\psi_L\rangle\,,$$

  the subscript i indicating that the operator acts on the ith qubit of $|\psi_L\rangle$.

Shor's Code: Error Correction

- After $\mathcal{E} |\psi_L\rangle$ is passed through the syndrome computation circuit, we obtain (by linearity)

$$\alpha_1 |\psi_L\rangle |\mathbf{0}\rangle + \alpha_2 X_i |\psi_L\rangle |\mathbf{s}_{X_i}\rangle + \alpha_3 Z_i |\psi_L\rangle |\mathbf{s}_{Z_i}\rangle + \alpha_4 X_i Z_i |\psi_L\rangle |\mathbf{s}_{X_i Z_i}\rangle$$

Shor's Code: Error Correction

- After $\mathcal{E}\,|\psi_L\rangle$ is passed through the syndrome computation circuit, we obtain (by linearity)

$$\alpha_1\,|\psi_L\rangle\,|\mathbf{0}\rangle + \alpha_2\,X_i\,|\psi_L\rangle\,|\mathbf{s}_{X_i}\rangle + \alpha_3\,Z_i\,|\psi_L\rangle\,|\mathbf{s}_{Z_i}\rangle + \alpha_4\,X_iZ_i\,|\psi_L\rangle\,|\mathbf{s}_{X_iZ_i}\rangle$$

- Measuring the syndrome qubits $|\mathbf{s}\rangle$ yields

Outcome	Post-measurement $\mathcal{E}\,|\psi_L\rangle$	Probability
$\mathbf{0}$	$|\psi_L\rangle$	$|\alpha_1|^2$
$\mathbf{s}_{X_i}$	$X_i\,|\psi_L\rangle$	$|\alpha_2|^2$
$\mathbf{s}_{Z_i}$	$Z_i\,|\psi_L\rangle$	$|\alpha_3|^2$
$\mathbf{s}_{X_iZ_i}$	$X_iZ_i\,|\psi_L\rangle$	$|\alpha_4|^2$

- The measurement outcome identifies the error operator present in the post-measurement state, and its effect can then be reversed.

Discretization of Errors

Shor's code illustrates the principle of discretization of errors:

> *to correct an arbitrary unitary error operator, it suffices to ensure that the basis errors I_2, X, Z and XZ can be corrected.*

Quantum Stabilizer Codes

The Pauli Matrices

- The four Pauli matrices

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

  form an orthonormal basis of $\mathbb{C}^{2\times 2}$ with respect to the inner product $(A, B) := \mathrm{tr}(A^\dagger B)$.

- Some useful properties:
  - $Y = iXZ \quad (i = \sqrt{-1})$
  - $\mathrm{tr}(X) = \mathrm{tr}(Y) = \mathrm{tr}(Z) = 0$ (traceless property)
  - $X^2 = Y^2 = Z^2 = I$ (involution)
  - $XY = -YX, \quad XZ = -ZX, \quad YZ = -ZY.$
    (anti-commutativity)
  - X, Y and Z all have eigenvalues $+1, -1$.

The Pauli group $\mathcal{P}_n$

$$\mathcal{P}_n := \{ i^\ell \cdot M_1 \otimes \cdots \otimes M_n : M_j \in \{I, X, Y, Z\}, \ell \in \{0, 1, 2, 3\} \}$$

- $\mathcal{P}_n$ is a subgroup of the multiplicative group, $\mathcal{U}(N)$, consisting of $N \times N$ unitary matrices ($N = 2^n$).
- $(M_1 \otimes \cdots \otimes M_n)(M_1' \otimes \cdots \otimes M_n') = M_1 M_1' \otimes \cdots \otimes M_n M_n'$.
- $\mathcal{P}_n$ is non-abelian; for example, $XZ = -ZX$.
- Any two elements of $\mathcal{P}_n$ either commute or anti-commute: either $MM' = M'M$ or $MM' = -M'M$.

Linear Algebraic Properties of $M_1 \otimes \cdots \otimes M_n$

- $M_1 \otimes \cdots \otimes M_n$, with $M_j \in \{I, X, Y, Z\}\,\forall j$, is Hermitian.
- $\mathrm{tr}(M_1 \otimes \cdots \otimes M_n) = \begin{cases} N\ (= 2^n) & \text{if } M_j = I \text{ for all } j \\ 0 & \text{otherwise} \end{cases}$
- Other than when $M_j = I$ for all j, the matrix $M_1 \otimes \cdots \otimes M_n$ has $N/2$ eigenvalues equal to $+1$ and $N/2$ eigenvalues equal to -1.

Linear Algebraic Properties of $M_1 \otimes \cdots \otimes M_n$

- $M_1 \otimes \cdots \otimes M_n$, with $M_j \in \{I, X, Y, Z\}\ \forall j$, is Hermitian.

- $\mathrm{tr}(M_1 \otimes \cdots \otimes M_n) = \begin{cases} N\ (= 2^n) & \text{if } M_j = I \text{ for all } j \\ 0 & \text{otherwise} \end{cases}$

- Other than when $M_j = I$ for all j, the matrix $M_1 \otimes \cdots \otimes M_n$ has $N/2$ eigenvalues equal to $+1$ and $N/2$ eigenvalues equal to -1.

- The 4^n matrices $M_1 \otimes \cdots \otimes M_n$, with $M_j \in \{I, X, Y, Z\}\ \forall j$, form an ON basis of $\mathbb{C}^{N \times N}$, with respect to the inner product $(A, B) = \mathrm{tr}(A^\dagger B)$.

Stabilizers

Daniel Gottesman, PhD Thesis, Caltech, 1997

For $\mathcal{S}$ a subgroup of $\mathcal{P}_n$, define the subspace of $\mathbb{C}^N$ stabilized by $\mathcal{S}$ to be the set of all n-qubit states $|\psi\rangle$ that are invariant under every Pauli operator in $\mathcal{S}$:

$$\mathcal{Q}_{\mathcal{S}} \; := \; \{|\psi\rangle : M\,|\psi\rangle = |\psi\rangle \;\text{ for all } M \in \mathcal{S}\}$$

- In other words, $\mathcal{Q}_{\mathcal{S}}$ is the common $+1$-eigenspace of all $M \in \mathcal{S}$.
- Any $M \in \mathcal{S}$ is called a stabilizer of $\mathcal{Q}_{\mathcal{S}}$.

Stabilizers

Daniel Gottesman, PhD Thesis, Caltech, 1997

For $\mathcal{S}$ a subgroup of $\mathcal{P}_n$, define the subspace of $\mathbb{C}^N$ stabilized by $\mathcal{S}$ to be the set of all n-qubit states $|\psi\rangle$ that are invariant under every Pauli operator in $\mathcal{S}$:

$$\mathcal{Q}_{\mathcal{S}} \;:=\; \{|\psi\rangle : M\,|\psi\rangle = |\psi\rangle \text{ for all } M \in \mathcal{S}\}$$

- In other words, $\mathcal{Q}_{\mathcal{S}}$ is the common $+1$-eigenspace of all $M \in \mathcal{S}$.
- Any $M \in \mathcal{S}$ is called a stabilizer of $\mathcal{Q}_{\mathcal{S}}$.
- Example: For $\mathcal{S} = \langle I \otimes Z \otimes Z,\; Z \otimes Z \otimes I\rangle = \{I \otimes I \otimes I,\; I \otimes Z \otimes Z,\; Z \otimes I \otimes Z,\; Z \otimes Z \otimes I\}$,

$$\mathcal{Q}_{\mathcal{S}} = \mathrm{span}(|000\rangle\,, |111\rangle).$$

Quantum Stabilizer Code

- If $\mathcal{S}$ is non-abelian or $-I_N \in \mathcal{S}$, then $\mathcal{Q}_{\mathcal{S}} = \{\mathbf{0}\}$.

Quantum Stabilizer Code

- If $\mathcal{S}$ is non-abelian or $-I_N \in \mathcal{S}$, then $\mathcal{Q}_\mathcal{S} = \{\mathbf{0}\}$.

Theorem

Let $\mathcal{S}$ be an abelian subgroup of $\mathcal{P}_n$ such that $-I_N \notin \mathcal{S}$. Then,

$$\dim \mathcal{Q}_\mathcal{S} = \frac{2^n}{|\mathcal{S}|}.$$

In particular, $\dim \mathcal{Q}_\mathcal{S} \geq 1$.

- A non-trivial $\mathcal{Q}_\mathcal{S}$ is referred to as a quantum stabilizer code.

Quantum Stabilizer Code

- If $\mathcal{S}$ is non-abelian or $-I_N \in \mathcal{S}$, then $\mathcal{Q}_{\mathcal{S}} = \{\mathbf{0}\}$.

Theorem

Let $\mathcal{S}$ be an abelian subgroup of $\mathcal{P}_n$ such that $-I_N \notin \mathcal{S}$. Then,

$$\dim \mathcal{Q}_{\mathcal{S}} = \frac{2^n}{|\mathcal{S}|}.$$

In particular, $\dim \mathcal{Q}_{\mathcal{S}} \geq 1$*.*

- A non-trivial $\mathcal{Q}_{\mathcal{S}}$ is referred to as a quantum stabilizer code.

From now onwards, we will use the term "stabilizer group" to mean an abelian subgroup of $\mathcal{P}_n$ that does not contain $-I_N$.

Stabilizer Groups

Let $\mathcal{S}$ be a stabilizer group.

- The elements in $\mathcal{S}$ are all of the form $\pm M_1 \otimes \cdots \otimes M_n$ with $M_j \in \{I, X, Y, Z\}$ for all j.

  The sign in front can either be $+$ or $-$, but not both.

Stabilizer Groups

Let $\mathcal{S}$ be a stabilizer group.

- The elements in $\mathcal{S}$ are all of the form $\pm M_1 \otimes \cdots \otimes M_n$ with $M_j \in \{I, X, Y, Z\}$ for all j.

  The sign in front can either be $+$ or $-$, but not both.

- $\mathcal{S}$ can be completely specified by a set of independent generators: $\mathcal{S} = \langle g_1, g_2, \ldots, g_m \rangle$.

  This means that each $M \in \mathcal{S}$ is uniquely expressible as a product of the generators g_j:

  $$\mathcal{S} \overset{\text{1-1}}{\longleftrightarrow} \left\{ \prod_{j \in J} g_j : J \subseteq [m] \right\}.$$

  Consequently, $|\mathcal{S}| = 2^m$.

Stabilizer Groups

Let $\mathcal{S}$ be a stabilizer group.

- The elements in $\mathcal{S}$ are all of the form $\pm M_1 \otimes \cdots \otimes M_n$ with $M_j \in \{I, X, Y, Z\}$ for all j.

  The sign in front can either be $+$ or $-$, but not both.

- $\mathcal{S}$ can be completely specified by a set of independent generators: $\mathcal{S} = \langle g_1, g_2, \ldots, g_m \rangle$.

  This means that each $M \in \mathcal{S}$ is uniquely expressible as a product of the generators g_j:

  $$\mathcal{S} \overset{\text{1-1}}{\longleftrightarrow} \left\{ \prod_{j \in J} g_j : J \subseteq [m] \right\}.$$

  Consequently, $|\mathcal{S}| = 2^m$.

- $\dim \mathcal{Q}_{\mathcal{S}} = 2^{n-m}$.

Symplectic Notation

- A Pauli operator of the form $M = M_1 \otimes \cdots \otimes M_n$ has a useful binary vector representation:

$$[\mathbf{a} \mid \mathbf{b}] \; = \; [a_1, a_2, \ldots, a_n \mid b_1, b_2, \ldots, b_n]$$

with

$$(a_j, b_j) = \begin{cases} (0,0) & \text{if } M_j = I \\ (1,0) & \text{if } M_j = X \\ (0,1) & \text{if } M_j = Z \\ (1,1) & \text{if } M_j = Y \end{cases}$$

- We also write this as

$$M = X(\mathbf{a})Z(\mathbf{b}) = X(a_1 a_2 \ldots a_n)Z(b_1 b_2 \ldots b_n).$$

Symplectic Notation

- A Pauli operator of the form $M = M_1 \otimes \cdots \otimes M_n$ has a useful binary vector representation:

$$[\mathbf{a} \mid \mathbf{b}] \; = \; [a_1, a_2, \ldots, a_n \mid b_1, b_2, \ldots, b_n]$$

with

$$(a_j, b_j) = \begin{cases} (0,0) & \text{if } M_j = I \\ (1,0) & \text{if } M_j = X \\ (0,1) & \text{if } M_j = Z \\ (1,1) & \text{if } M_j = Y \end{cases}$$

- We also write this as

$$M = X(\mathbf{a})Z(\mathbf{b}) = X(a_1 a_2 \ldots a_n)Z(b_1 b_2 \ldots b_n).$$

- Example: $M = Y \otimes Z \otimes I \otimes Y \otimes X$ has the vector representation $[1,0,0,1,1 \mid 1,1,0,1,0]$. We also write this as

$$M = X(10011)Z(11010)$$

Utility of Symplectic Notation

Let $M = X(\mathbf{a})Z(\mathbf{b})$ and $M' = X(\mathbf{a}')Z(\mathbf{b}')$.

- $MM' = (-1)^{\mathbf{a}' \cdot \mathbf{b}} X(\mathbf{a} \oplus \mathbf{a}')Z(\mathbf{b} \oplus \mathbf{b}')$

Utility of Symplectic Notation

Let $M = X(\mathbf{a})Z(\mathbf{b})$ and $M' = X(\mathbf{a}')Z(\mathbf{b}')$.

- $MM' = (-1)^{\mathbf{a}'\cdot\mathbf{b}} X(\mathbf{a} \oplus \mathbf{a}')Z(\mathbf{b} \oplus \mathbf{b}')$
  $M'M = (-1)^{\mathbf{a}\cdot\mathbf{b}'} X(\mathbf{a} \oplus \mathbf{a}')Z(\mathbf{b} \oplus \mathbf{b}')$.

- Thus, $M = X(\mathbf{a})Z(\mathbf{b})$ and $M' = X(\mathbf{a}')Z(\mathbf{b}')$ commute if and only if $(-1)^{\mathbf{a}'\cdot\mathbf{b}} = (-1)^{\mathbf{a}\cdot\mathbf{b}'}$, or equivalently,

$$\mathbf{a}' \cdot \mathbf{b} \equiv \mathbf{a} \cdot \mathbf{b}' \pmod 2$$

Symplectic Inner Product

- The symplectic inner product between $[\mathbf{a} \mid \mathbf{b}]$ and $[\mathbf{a}' \mid \mathbf{b}']$ is defined as

$$\langle [\mathbf{a}|\mathbf{b}] \mid [\mathbf{a}'|\mathbf{b}'] \rangle_{\mathrm{s}} \;:=\; \mathbf{a}' \cdot \mathbf{b} - \mathbf{a} \cdot \mathbf{b}'$$

- Thus, $M = X(\mathbf{a})Z(\mathbf{b})$ and $M' = X(\mathbf{a}')Z(\mathbf{b}')$ commute if and only if $\langle [\mathbf{a}|\mathbf{b}] \mid [\mathbf{a}'|\mathbf{b}'] \rangle_{\mathrm{s}} \equiv 0 \pmod 2$.

- Example: $M = Y \otimes Z \otimes I \otimes Y \otimes X = X(10011)Z(11010)$ $M' = Z \otimes I \otimes Y \otimes I \otimes X = X(00101)Z(10100)$.

  The symplectic inner product between $[10011 \mid 11010]$ and $[00101 \mid 10100]$ is $1 \pmod 2$, so M and M' anti-commute.

Check Matrix

Let $\mathcal{S} = \langle g_1, g_2, \ldots, g_m \rangle$ be a stabilizer group in $\mathcal{P}_n$.

Let $g_\ell = X(\mathbf{a}^{(\ell)})Z(\mathbf{b}^{(\ell)})$, $\ell = 1, 2, \ldots, m$.

- The check matrix representation of this set of generators is a $m \times 2n$ matrix H whose ℓ-th row is $[\mathbf{a}^{(\ell)} \mid \mathbf{b}^{(\ell)}]$.

- Example: $\mathcal{S} = \langle I \otimes Z \otimes Z,\ Z \otimes Z \otimes I \rangle$ has the check matrix

$$H = \left[\begin{array}{ccc|ccc} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{array}\right]$$

Check Matrix

Let $\mathcal{S} = \langle g_1, g_2, \ldots, g_m \rangle$ be a stabilizer group in $\mathcal{P}_n$.

Let $g_\ell = X(\mathbf{a}^{(\ell)})Z(\mathbf{b}^{(\ell)})$, $\ell = 1, 2, \ldots, m$.

- The check matrix representation of this set of generators is a $m \times 2n$ matrix H whose ℓ-th row is $[\mathbf{a}^{(\ell)} \mid \mathbf{b}^{(\ell)}]$.

- Example: $\mathcal{S} = \langle I \otimes Z \otimes Z,\ Z \otimes Z \otimes I \rangle$ has the check matrix

$$H = \begin{bmatrix} 0 & 0 & 0 & | & 0 & 1 & 1 \\ 0 & 0 & 0 & | & 1 & 1 & 0 \end{bmatrix}$$

- Generators $g_1, g_2, \ldots, g_m$ are independent if and only if the corresponding check matrix has rank m.

A Prescription for Constructing Quantum Stabilizer Codes

1. Pick m linearly independent vectors

$$[\mathbf{a}^{(1)}, \mathbf{b}^{(1)}], [\mathbf{a}^{(2)}, \mathbf{b}^{(2)}], \ldots, [\mathbf{a}^{(m)}, \mathbf{b}^{(m)}] \in \{0,1\}^{2n}$$

   such that

$$\langle [\mathbf{a}^{(k)}, \mathbf{b}^{(k)}] \mid [\mathbf{a}^{(\ell)}, \mathbf{b}^{(\ell)}] \rangle_{\mathrm{s}} \equiv 0 \pmod 2 \quad \text{for all } k, \ell$$

2. Set up the stabilizer generators $g_j = X(\mathbf{a}^{(j)})Z(\mathbf{b}^{(j)})$, $j = 1, 2, \ldots, m$, and the stabilizer group $\mathcal{S} = \langle g_1, g_2, \ldots, g_m \rangle$.

The resulting n-qubit subspace $\mathcal{Q}_{\mathcal{S}}$ has dimension 2^{n-m}, so it can hold $n - m$ logical qubits.

We call $\mathcal{Q}_{\mathcal{S}}$ an $[[n, n-m]]_2$ quantum stabilizer code.

The Calderbank-Shor-Steane (CSS) Construction

Calderbank-Shor (1996), Steane (1996)

- Pick an $[n, k_1]$ (classical) binary linear code $\mathcal{C}_1$ and an $[n, k_2]$ binary linear code $\mathcal{C}_2$ such that $\mathcal{C}_2^{\perp} \subseteq \mathcal{C}_1$.

- Let H_i be an $(n-k_i) \times n$ parity-check matrix for $\mathcal{C}_i$. Note that

$$\mathcal{C}_2^{\perp} \subseteq \mathcal{C}_1 \iff H_1 H_2^T = 0 \pmod 2$$

- Set $m := (n-k_1) + (n-k_2)$ and construct the $m \times 2n$ check matrix

$$H = \begin{bmatrix} H_1 & | & \mathbf{0} \\ - & - & - \\ \mathbf{0} & | & H_2 \end{bmatrix}$$

- By construction, the H matrix has rank m.

The Calderbank-Shor-Steane (CSS) Construction

Calderbank-Shor (1996), Steane (1996)

- It is easy to check that the symplectic inner product between any pair of rows of H is equal to 0 (mod 2):
  - $\langle \cdot | \cdot \rangle_{\mathrm{s}} = 0$ for any pair of rows from the top half
  - $\langle \cdot | \cdot \rangle_{\mathrm{s}} = 0$ for any pair of rows from the bottom half
  - the condition $H_1 H_2^T = 0$ ensures that $\langle \cdot | \cdot \rangle_{\mathrm{s}} = 0$ when one row comes from the top half and the other from the bottom half

The Calderbank-Shor-Steane (CSS) Construction

Calderbank-Shor (1996), Steane (1996)

- It is easy to check that the symplectic inner product between any pair of rows of H is equal to $0 \pmod 2$:
  - $\langle \cdot | \cdot \rangle_{\mathrm{s}} = 0$ for any pair of rows from the top half
  - $\langle \cdot | \cdot \rangle_{\mathrm{s}} = 0$ for any pair of rows from the bottom half
  - the condition $H_1 H_2^T = 0$ ensures that $\langle \cdot | \cdot \rangle_{\mathrm{s}} = 0$ when one row comes from the top half and the other from the bottom half
- The rows of H yield m independent generators of a stabilizer group $\mathcal{S}$.
- The associated n-qubit subspace $\mathcal{Q}_{\mathcal{S}}$ is an $[[n, k_1 + k_2 - n]]_2$ quantum stabilizer code, termed a CSS code.

Example: The $[[7,1]]_2$ Steane Code

- Take $\mathcal{C}_1 = \mathcal{C}_2 = [7,4]$ binary Hamming code, with parity-check matrix

$$H_1 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

  It is easily verified that $H_1 H_1^T = 0 \pmod 2$.

- Applying the CSS construction results in the check matrix

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & | & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & | & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & | & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ - & - & - & - & - & - & - & - & - & - & - & - & - & - & - \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & | & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & | & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & | & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Example: The $[[7,1]]_2$ Steane Code

- The stabilizer generators correponding to the rows of the check matrix are

$$
\begin{aligned}
g_1 &= X \otimes X \otimes I \otimes X \otimes X \otimes I \otimes I \\
g_2 &= X \otimes I \otimes X \otimes X \otimes I \otimes X \otimes I \\
g_3 &= I \otimes X \otimes X \otimes X \otimes I \otimes I \otimes X \\
\\
g_4 &= Z \otimes Z \otimes I \otimes Z \otimes Z \otimes I \otimes I \\
g_5 &= Z \otimes I \otimes Z \otimes Z \otimes I \otimes Z \otimes I \\
g_6 &= I \otimes Z \otimes Z \otimes Z \otimes I \otimes I \otimes Z
\end{aligned}
$$

- The stabilizer group $\mathcal{S}$ generated by these gives rise to a $[[7,1]]_2$ quantum stabilizer code called the Steane code.

Example: Shor's Code

Shor's code is also a CSS code obtained from the following matrices:

$$H_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$H_2 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

-

The Centralizer of a Stabilizer Group

Let $\mathcal{S}$ be a stabilizer group in $\mathcal{P}_n$.

Definition

The centralizer of $\mathcal{S}$ in $\mathcal{P}_n$ is the set of all operators in $\mathcal{P}_n$ that commute with every $M \in \mathcal{S}$; denoted by $\mathcal{Z}(\mathcal{S})$.

- Note that $\mathcal{S} \subseteq \mathcal{Z}(\mathcal{S})$.
- It can be shown that $|\mathcal{Z}(\mathcal{S})| = \dfrac{2^{2n}}{|\mathcal{S}|}$.

The Centralizer of a Stabilizer Group

Let $\mathcal{S}$ be a stabilizer group in $\mathcal{P}_n$.

Definition

The centralizer of $\mathcal{S}$ in $\mathcal{P}_n$ is the set of all operators in $\mathcal{P}_n$ that commute with every $M \in \mathcal{S}$; denoted by $\mathcal{Z}(\mathcal{S})$.

- Note that $\mathcal{S} \subseteq \mathcal{Z}(\mathcal{S})$.
- It can be shown that $|\mathcal{Z}(\mathcal{S})| = \dfrac{2^{2n}}{|\mathcal{S}|}$.

Example: $\mathcal{S} = \langle I \otimes Z \otimes Z,\ Z \otimes Z \otimes I \rangle$.
$IZZ = X(000)Z(011)$ and $ZZI = X(000)Z(110)$.

The centralizer, $\mathcal{Z}(\mathcal{S}) = \{X(000)Z(***), X(111)Z(***)\}$.

Error Correction

Let $\mathcal{Q}$ be an $[[n, k]]_2$ quantum stabilizer code.

Definition (informal):
A set of unitary error operators $\mathcal{E} \subseteq \mathcal{U}(N)$ is said to be correctable by $\mathcal{Q}$ if there exists a recovery operation $\mathcal{R}$ such that for all $|\psi\rangle \in \mathcal{Q}$ and all $E \in \mathcal{E}$, we can recover $|\psi\rangle$ by applying $\mathcal{R}$ to $E\,|\psi\rangle$.

$$|\psi\rangle \;—\!\!\boxed{\mathcal{E}}\!\!—\!\!\boxed{\mathcal{R}}\!\!—\; |\psi\rangle$$

Error Correction

Let $\mathcal{Q}$ be an $[[n,k]]_2$ quantum stabilizer code.

Definition (informal):
A set of unitary error operators $\mathcal{E} \subseteq \mathcal{U}(N)$ is said to be correctable by $\mathcal{Q}$ if there exists a recovery operation $\mathcal{R}$ such that for all $|\psi\rangle \in \mathcal{Q}$ and all $E \in \mathcal{E}$, we can recover $|\psi\rangle$ by applying $\mathcal{R}$ to $E\,|\psi\rangle$.

$$|\psi\rangle \;\text{———}\; \boxed{\mathcal{E}} \;\text{———}\; \boxed{\mathcal{R}} \;\text{———}\; |\psi\rangle$$

- Recall that the Pauli matrices $M_1 \otimes \cdots \otimes M_n$, with $M_j \in \{I, X, Y, Z\}$ for all j, form a basis of $\mathbb{C}^{N \times N}$.
- So, the principle of discretization of errors allows us to focus on correcting error operators that come from $\mathcal{P}_n$.

Error Correction within $\mathcal{P}_n$

Let $\mathcal{S}$ be a stabilizer group within $\mathcal{P}_n$, with $\mathcal{Q}_\mathcal{S}$ its quantum stabilizer code.

Theorem

A subset $\mathcal{E} \subseteq \mathcal{P}_n$ is correctable by $\mathcal{Q}_\mathcal{S}$ if and only if

$$E_1^\dagger E_2 \notin \mathcal{Z}(\mathcal{S}) \setminus \mathcal{S} \quad \textit{for all } E_1, E_2 \in \mathcal{E}.$$

Minimum Distance

- The symplectic weight of a Pauli operator $M = i^\ell M_1 \otimes \cdots \otimes M_n$ is defined as

$$\mathrm{wt_s}(M) \ = \ \#\{j : M_j \neq I\}.$$

- For an $[[n,k]]_2$ quantum stabilizer code $\mathcal{Q}_\mathcal{S}$ with $k > 0$, we define the minimum distance to be

$$d_{\mathsf{min}}(\mathcal{Q}_\mathcal{S}) \ = \ \min\{\mathrm{wt_s}(M) : M \in \mathcal{Z}(\mathcal{S}) \setminus \mathcal{S}\}.$$

- An $[[n,k,d]]_2$ quantum stabilizer code is a 2^k-dimensional subspace of $\mathbb{C}^{2^n}$, with $d_{\mathsf{min}} = d$.

Example: $\mathcal{S} = \langle I \otimes Z \otimes Z,\ Z \otimes Z \otimes I \rangle$

For $\mathcal{S} = \langle I \otimes Z \otimes Z,\ Z \otimes Z \otimes I \rangle$, recall that

- $\mathcal{Q}_{\mathcal{S}} = \text{span}(|000\rangle, |111\rangle)$, so that $\dim(\mathcal{Q}_{\mathcal{S}}) = 2^1$, i.e., $k = 1$.
- $\mathcal{Z}(\mathcal{S}) = \{X(000)Z(***), X(111)Z(***)\}$

Example: $\mathcal{S} = \langle I \otimes Z \otimes Z,\ Z \otimes Z \otimes I \rangle$

For $\mathcal{S} = \langle I \otimes Z \otimes Z,\ Z \otimes Z \otimes I \rangle$, recall that

- $\mathcal{Q}_{\mathcal{S}} = \text{span}(|000\rangle, |111\rangle)$, so that $\dim(\mathcal{Q}_{\mathcal{S}}) = 2^1$, i.e., $k = 1$.
- $\mathcal{Z}(\mathcal{S}) = \{X(000)Z(***), X(111)Z(***)\}$

Then,

- $d_{\min}(\mathcal{Q}_{\mathcal{S}}) = 1$, since $I \otimes I \otimes Z \in \mathcal{Z}(\mathcal{S}) \setminus \mathcal{S}$.

Thus, $\mathcal{Q}_{\mathcal{S}}$ is a $[[3, 1, 1]]_2$ quantum stabilizer code.

Minimum Distance and Error Correction

Let $\mathcal{Q}_{\mathcal{S}}$ be an $[[n, k, d]]$ quantum stabilizer code, with $k > 0$.

Proposition: The set of error operators

$$\mathcal{E} = \{M \in \mathcal{P}_n : \mathrm{wt_s}(M) < d/2\}$$

is correctable by $\mathcal{Q}_{\mathcal{S}}$.

Proof:

- For any $E_1, E_2 \in \mathcal{E}$, we have

$$\mathrm{wt_s}(E_1^\dagger E_2) \;\leq\; \underbrace{\mathrm{wt_s}(E_1)}_{< d/2} + \underbrace{\mathrm{wt_s}(E_2)}_{< d/2} \;< d$$

- Since $d = \min\{\mathrm{wt_s}(M) : M \in \mathcal{Z}(\mathcal{S}) \setminus \mathcal{S}\}$, we find that $E_1^\dagger E_2 \neq \mathcal{Z}(\mathcal{S}) \setminus \mathcal{S}$. □

Minimum Distance of a CSS Code

Let $\mathcal{C}_1$ be an $[n, k_1]$ binary linear code and $\mathcal{C}_2$ an $[n, k_2]$ binary linear code such that $\mathcal{C}_2^\perp \subseteq \mathcal{C}_1$.

Let $\mathcal{Q}$ be the resulting $[[n, k_1 + k_2 - n]]_2$ CSS code.

- $d_{\min}(\mathcal{Q}) \; = \min\{d_1, d_2\}$, where

  $d_1 = \min\{w(\mathbf{c}) : \mathbf{c} \in \mathcal{C}_1 \setminus \mathcal{C}_2^\perp\}$ and $d_2 = \min\{w(\mathbf{c}) : \mathbf{c} \in \mathcal{C}_2 \setminus \mathcal{C}_1^\perp\}$

Minimum Distance of a CSS Code

Let $\mathcal{C}_1$ be an $[n, k_1]$ binary linear code and $\mathcal{C}_2$ an $[n, k_2]$ binary linear code such that $\mathcal{C}_2^{\perp} \subseteq \mathcal{C}_1$.

Let $\mathcal{Q}$ be the resulting $[[n, k_1 + k_2 - n]]_2$ CSS code.

- $d_{\min}(\mathcal{Q}) = \min\{d_1, d_2\}$, where

  $d_1 = \min\{w(\mathbf{c}) : \mathbf{c} \in \mathcal{C}_1 \setminus \mathcal{C}_2^{\perp}\}$ and $d_2 = \min\{w(\mathbf{c}) : \mathbf{c} \in \mathcal{C}_2 \setminus \mathcal{C}_1^{\perp}\}$

- Example: Recall that the Steane code is the CSS code constructed from $\mathcal{C}_1 = \mathcal{C}_2 = [7, 4]$ binary Hamming code.

  For the Hamming code $\mathcal{C}$, it can be verified that $\min\{w(\mathbf{c}) : \mathbf{c} \in \mathcal{C} \setminus \mathcal{C}^{\perp}\} = 3$.

  Therefore, the Steane code is a $[[7, 1, 3]]_2$ stabilizer code.

Minimum Distance of a CSS Code

Let $\mathcal{C}_1$ be an $[n, k_1]$ binary linear code and $\mathcal{C}_2$ an $[n, k_2]$ binary linear code such that $\mathcal{C}_2^{\perp} \subseteq \mathcal{C}_1$.

Let $\mathcal{Q}$ be the resulting $[[n, k_1 + k_2 - n]]_2$ CSS code.

- $d_{\min}(\mathcal{Q}) \; = \min\{d_1, d_2\}$, where

  $d_1 = \min\{w(\mathbf{c}) : \mathbf{c} \in \mathcal{C}_1 \setminus \mathcal{C}_2^{\perp}\}$ and $d_2 = \min\{w(\mathbf{c}) : \mathbf{c} \in \mathcal{C}_2 \setminus \mathcal{C}_1^{\perp}\}$

- Example: Recall that the Steane code is the CSS code constructed from $\mathcal{C}_1 = \mathcal{C}_2 = [7, 4]$ binary Hamming code.

  For the Hamming code $\mathcal{C}$, it can be verified that $\min\{w(\mathbf{c}) : \mathbf{c} \in \mathcal{C} \setminus \mathcal{C}^{\perp}\} = 3$.

  Therefore, the Steane code is a $[[7, 1, 3]]_2$ stabilizer code.

  It is, thus, single-error-correcting, with a better ratio of logical qubits to physical qubits than the $[[9, 1, 3]]_2$ Shor code.

Error Correction Via Syndromes

$\mathcal{S} = \langle g_1, g_2, \ldots, g_{n-k} \rangle$ with $\mathcal{Q}_{\mathcal{S}}$ an $[[n,k]]_2$ stabilizer code.

$\mathcal{E} \subset \mathcal{P}_n$ a set of errors s.t. $E_1^\dagger E_2 \notin \mathcal{Z}(\mathcal{S}) \setminus \mathcal{S}$ for all $E_1, E_2 \in \mathcal{E}$.

- Suppose that $|\psi\rangle \in \mathcal{Q}_{\mathcal{S}}$ is acted on by $E_1 \in \mathcal{E}$ to become $|\psi'\rangle = E_1 |\psi\rangle$.

$$|\psi\rangle \;-\!\!-\!\!\boxed{E_1}\!\!-\!\!-\; |\psi'\rangle$$

Error Correction Via Syndromes

$\mathcal{S} = \langle g_1, g_2, \ldots, g_{n-k} \rangle$ with $\mathcal{Q}_\mathcal{S}$ an $[[n,k]]_2$ stabilizer code.

$\mathcal{E} \subset \mathcal{P}_n$ a set of errors s.t. $E_1^\dagger E_2 \notin \mathcal{Z}(\mathcal{S}) \setminus \mathcal{S}$ for all $E_1, E_2 \in \mathcal{E}$.

- Suppose that $|\psi\rangle \in \mathcal{Q}_\mathcal{S}$ is acted on by $E_1 \in \mathcal{E}$ to become $|\psi'\rangle = E_1 |\psi\rangle$.

$$|\psi\rangle \;—\boxed{E_1}—\; |\psi'\rangle$$

- Define the syndrome of E_1 to be $\mathbf{s} = [s_1, s_2, \ldots, s_{n-k}]$, given by

$$s_\ell = \begin{cases} 0 & \text{if } E_1 \text{ commutes with } g_\ell \\ 1 & \text{if } E_1 \text{ anti-commutes with } g_\ell \end{cases}$$

for $\ell = 1, 2, \ldots, n-k$.

In other words, $E_1 g_\ell = (-1)^{s_\ell} g_\ell E_1$.

Error Correction Via Syndromes

- Assume, for now, that the syndrome **s** can be computed directly from $|\psi'\rangle$ without disturbing it.
- If the syndrome **s** uniquely identifies $E_1 \in \mathcal{E}$, then we simply apply $E_1^\dagger$ to $|\psi'\rangle$:

$$|\psi'\rangle \; \text{———} \boxed{E_1^\dagger} \text{———} \; |\psi\rangle$$

- On the other hand, suppose there are multiple error operators in $\mathcal{E}$ that have the same syndrome **s**.
  - If E_1, E_2 are two such operators, then $E_2^\dagger E_1$ commutes with all stabilizer generators g_ℓ:

$$\begin{aligned} E_2^\dagger E_1 g_\ell &= E_2^\dagger (-1)^{s_\ell} g_\ell E_1 \\ &= (-1)^{s_\ell} E_2^\dagger g_\ell E_1 \;=\; g_\ell E_2^\dagger E_1 \end{aligned}$$

  - Hence, $E_2^\dagger E_1$ is in $\mathcal{Z}(\mathcal{S})$.

Error Correction Via Syndromes

- Assume, for now, that the syndrome **s** can be computed directly from $|\psi'\rangle$ without disturbing it.
- If the syndrome **s** uniquely identifies $E_1 \in \mathcal{E}$, then we simply apply $E_1^\dagger$ to $|\psi'\rangle$:

$$|\psi'\rangle \;—\boxed{E_1^\dagger}—\; |\psi\rangle$$

- On the other hand, suppose there are multiple error operators in $\mathcal{E}$ that have the same syndrome **s**.
  - If E_1, E_2 are two such operators, then $E_2^\dagger E_1$ commutes with all stabilizer generators g_ℓ:

$$\begin{aligned} E_2^\dagger E_1 g_\ell &= E_2^\dagger (-1)^{s_\ell} g_\ell E_1 \\ &= (-1)^{s_\ell} E_2^\dagger g_\ell E_1 \;=\; g_\ell E_2^\dagger E_1 \end{aligned}$$

  - Hence, $E_2^\dagger E_1$ is in $\mathcal{Z}(\mathcal{S})$.
  - However, by our assumption on $\mathcal{E}$, we have $E_2^\dagger E_1 \notin \mathcal{Z}(\mathcal{S}) \setminus \mathcal{S}$. Hence, $E_2^\dagger E_1 \in \mathcal{S}$.

Error Correction Via Syndromes

- So, if there are multiple error operators in $\mathcal{E}$ that have the same syndrome **s**, pick any one of them, say E_2, and apply $E_2^\dagger$ to $|\psi'\rangle$!

  $$|\psi'\rangle \;\; —\boxed{E_2^\dagger}— \;\; |\psi\rangle$$

  The reason this works is that

  $$E_2^\dagger |\psi'\rangle \;=\; \underbrace{E_2^\dagger E_1}_{\in \mathcal{S}} |\psi\rangle \;=\; |\psi\rangle .$$

Determining the Syndrome from $|\psi'\rangle$

- Key observation:

$$
\begin{aligned}
g_\ell |\psi'\rangle \;=\; g_\ell E_1 |\psi\rangle \;&=\; (-1)^{s_\ell} E_1 g_\ell |\psi\rangle \\
&=\; (-1)^{s_\ell} E_1 |\psi\rangle \;=\; (-1)^{s_\ell} |\psi'\rangle
\end{aligned}
$$

Thus, $|\psi'\rangle$ is in the $(-1)^{s_\ell}$-eigenspace of g_ℓ.

Determining the Syndrome from $|\psi'\rangle$

- Key observation:

$$\begin{aligned} g_\ell |\psi'\rangle &= g_\ell E_1 |\psi\rangle = (-1)^{s_\ell} E_1 g_\ell |\psi\rangle \\ &= (-1)^{s_\ell} E_1 |\psi\rangle = (-1)^{s_\ell} |\psi'\rangle \end{aligned}$$

  Thus, $|\psi'\rangle$ is in the $(-1)^{s_\ell}$-eigenspace of g_ℓ.

- If we measure $|\psi'\rangle$ using the observable g_ℓ, then
  - the measurement outcome is $(-1)^{s_\ell}$, with probability 1;
  - the post-measurement state remains $|\psi'\rangle$.

  Thus, the syndrome bit s_ℓ can be recovered from the measurement outcome without affecting $|\psi'\rangle$.

Error Correction Via Syndromes: Summary

$$|\psi\rangle \;\text{---}\boxed{E_1}\text{---}\; |\psi'\rangle$$

1. Determine the syndrome $\mathbf{s}$ by measuring $|\psi'\rangle$ in each of the observables g_ℓ, $\ell = 1, 2, \ldots, n - k$.

2. Identify an error operator, E_2, that has syndrome equal to $\mathbf{s}$.

3. Apply $E_2^\dagger$ to $|\psi'\rangle$:

$$|\psi'\rangle \;\text{---}\boxed{E_2^\dagger}\text{---}\; |\psi\rangle$$

Quantum Channels

The performance of stabilizer codes, specifically CSS codes, is often evaluated over one of two types of quantum channels:

- Depolarizing noise: Each qubit undergoes an error according to the following probabilities (independent across qubits):
  - $(1-p)$: I (i.e., no error)
  - $p/3$: X error
  - $p/3$: Y error
  - $p/3$: Z error

- Independent X-Z noise: Single-qubit errors occur according to the following probabilities (again, independent across qubits):
  - $(1-p)^2$: I (i.e., no error)
  - $p(1-p)$: X error
  - p^2: Y (i.e., XZ) error
  - $p(1-p)$: Z error

Maximum-Likelihood (ML) Decoding

Let $\mathcal{S}$ be a stabilizer subgroup of $\mathcal{P}_n$, with $\mathcal{Q}_\mathcal{S}$ the corresponding stabilizer code.

$$\mathcal{Q}_\mathcal{S} \ni |\psi\rangle \; \text{———} \boxed{\mathcal{E}} \text{———} \; |\psi'\rangle$$

Maximum-Likelihood (ML) Decoding

Let $\mathcal{S}$ be a stabilizer subgroup of $\mathcal{P}_n$, with $\mathcal{Q}_\mathcal{S}$ the corresponding stabilizer code.

$$\mathcal{Q}_\mathcal{S} \ni |\psi\rangle \;\longrightarrow\!\boxed{\mathcal{E}}\!\longrightarrow\; |\psi'\rangle$$

Maximum-Likelihood Decoding:

- Measure $|\psi'\rangle$ to determine the syndrome $\mathbf{s}$.
- The syndrome $\mathbf{s}$ uniquely identifies the coset, $\mathcal{W}$, of $\mathcal{Z}(\mathcal{S})$ within $\mathcal{P}_n$ which contains the true error E.
- Find the coset, $\mathcal{T}$, of $\mathcal{S}$ with the largest probability that is contained in $\mathcal{W}$, and pick *any* $\tilde{E} \in \mathcal{T}$:

$$|\psi'\rangle \;\longrightarrow\!\boxed{\tilde{E}^\dagger}\!\longrightarrow\; |\hat{\psi}\rangle$$

Selected Families of Quantum Codes

- Topological codes
  - Toric codes
  - Surface codes
  - Colour codes
- Quantum LDPC codes
  - Hypergraph product codes
  - Lifted product codes
  - Quantum Tanner codes
- Subsystem codes
- Floquet codes
- Entanglement-assisted codes
- Bosonic codes
  - Gottesman-Kitaev-Preskill (GKP) codes
  - Cat codes
  - Fock-state codes

Bibliography

[1] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, 10th Anniversary Edition, Cambridge Univ. Press, 2010.

[2] D.A. Lidar and T.A. Brun (eds.), *Quantum Error Correction*, Cambridge University Press, 2013.

[3] Daniel Gottesman, *Stabilizer Codes and Quantum Error Correction*, PhD thesis, Caltech, 1997.

[4] John Preskill, Lecture notes on quantum error correcting codes, Physics 219 course website, Caltech.

[5] Dan Browne, Lectures on topological codes and quantum computation, University College London.

[6] Error Correction Zoo: `https://errorcorrectionzoo.org/`