Quantum error correction

errorcorrectionzoo.org

We know from information theory that error correction is an important concept

* lossy communication
* lossy computation
* Damaged storage

data

$$\underline{x} \xrightarrow{\text{errors occur}} \underline{y}$$

ECCs provide a way to recover x from y when certain errors occur!

Simplest example (Repetition code)

Single bit $x \in \{0,1\}$

Noisy channel

$$x \xrightarrow{p} x \oplus 1$$
$$x \xrightarrow{1-p} x$$

With probability p we lose our information about x.

Idea: add redundancy (encoding)

logical bit

codewords (physical bits)

$$0 \longmapsto 000$$
$$1 \longmapsto 111$$

What happens if we send the physical bits through the channel?

If $x=0$

Output	Prob
000	$(1-p)^3$
001	$p(1-p)^2$
010	$p(1-p)^2$
100	$p(1-p)^2$
...	$O(p^2)$

Output	Prob
111	$(1-p)^3$
110	$p(1-p)^2$
101	
011	$\vdots$
...	negl

Decoding:

$$\begin{matrix}000\\001\\010\\100\end{matrix} \longmapsto 0 \qquad \begin{matrix}111\\110\\101\\011\end{matrix} \longmapsto 1$$

Probability we make a mistake is $p^3 + 3p^2(1-p)$

$$= 3p^2 - 2p^3 < p$$

whenever $\underline{\underline{p < \frac{1}{2}}}$ we get an advantage.

By adding redundancy to our message we could protect it from errors.

A first attempt at QEC

In quantum systems we also need error correction (they're very noisy!)

A naive attempt would be to replicate the rep-code

$$|\psi\rangle \longmapsto |\psi\rangle|\psi\rangle|\psi\rangle$$

But there are issues here (What can you think of?)

1) No cloning: if $|\psi\rangle$ is unknown then there's no way we can reliably copy it.
2) Detecting errors requires observing the string classically. Measurements disturb states (Problem?)
3) There are a lot more possible errors for quantum (a continuum) e.g. $R_\theta = \begin{pmatrix}1 & 0\\ 0 & e^{i\theta}\end{pmatrix}$ can occur.

<u>Our first scheme (Dealing with bitflip errors)</u> Recall $X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ bitflip in $\{|0\rangle, |1\rangle\}$ basis.

Suppose for the moment we only care about X errors. So we have a qubit channel

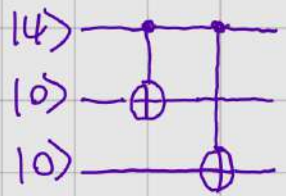
$$|\nu\rangle \xrightarrow{p} X|\nu\rangle$$
$$|\nu\rangle \xrightarrow{1-p} |\nu\rangle$$

We make the following encoding

$$|0\rangle \longmapsto |000\rangle$$
$$|1\rangle \longmapsto |111\rangle$$

Why does this not violate no-cloning?

This can be done with a circuit



If $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

then circuit outputs

$$\alpha|000\rangle + \beta|111\rangle$$

entangled state if $\alpha \neq 0 \neq \beta$

Now we pass each qubit through the noisy channel:

Assuming errors act independently:

Prob	State
$(1-p)^3$	$\alpha|000\rangle + \beta|111\rangle$
$p(1-p)^2$	$\alpha|100\rangle + \beta|011\rangle$
$p(1-p)^2$	$\alpha|010\rangle + \beta|101\rangle$
$p(1-p)^2$	$\alpha|001\rangle + \beta|110\rangle$
negl	

What can we do now?

States all live in orthogonal subspaces and so can be reliably distinguished!

$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$ → No error

$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$ → Qubit 1 error

$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$ → Qubit 2 error

$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$ → Qubit 3 error

1) These measurements will perfectly distinguish the different errors

E.g. $\langle\psi|P_i|\psi\rangle = \delta_{i0}$ $\quad\langle\psi|(X\otimes\mathbb{1}\otimes\mathbb{1})P_i(X\otimes\mathbb{1}\otimes\mathbb{1})|\psi\rangle = \delta_{i1}$

2) The measurement does not disturb the underlying state (Why?)

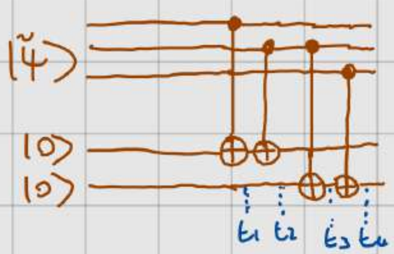
$\Rightarrow$ The measurement detects which (if any) X error occured and when we get outcome i the state after measurement is

$$X_i|\psi\rangle$$

where
$$X_0 = \mathbb{1}\otimes\mathbb{1}\otimes\mathbb{1}$$
$$X_1 = X\otimes\mathbb{1}\otimes\mathbb{1}$$
$$X_2 = \mathbb{1}\otimes X\otimes\mathbb{1}$$
$$X_3 = \mathbb{1}\otimes\mathbb{1}\otimes X$$

So we can correct the error we detected!

A circuit viewpoint on error detection



Recall CNOT $|0\rangle\langle 0|\otimes\mathbb{1} + |1\rangle\langle 1|\otimes X$

$|\tilde\psi\rangle \in \{|\psi\rangle, X_1|\psi\rangle, X_2|\psi\rangle, X_3|\psi\rangle\}$

$|\tilde\psi\rangle = \alpha|abc\rangle + \beta|xyz\rangle$

At t_1: $\quad\alpha|abc\rangle|a\rangle|0\rangle + \beta|xyz\rangle|x\rangle|0\rangle$

t_2: $\quad\alpha|abc\rangle|a\oplus b\rangle|0\rangle + \beta|xyz\rangle|x\oplus y\rangle|0\rangle$

$\vdots$

t_4 $\quad\alpha|abc\rangle|a\oplus b\rangle|b\oplus c\rangle + \beta|xyz\rangle|x\oplus y\rangle|y\oplus z\rangle$

The two extra states encode the parity of pairs of qubits.

1) Measure Qubit 4 in computational basis
- $0 \rightarrow$ No error on 1st 2 qubits
- $1 \rightarrow$ Qubit 1 or Qubit 2 has error

2) Measure Qubit 5 in computational basis
- $0 \rightarrow$ No error on 2nd 2 qubits
- $1 \rightarrow$ Qubit 2 or qubit 3 has error

Outcome	Error
$(0,0)$	$\mathbb{1}$
$(0,1)$	X_3
$(1,0)$	X_1
$(1,1)$	X_2

↖ Error Syndrome

2 bits of information sufficient to detect and correct the errors.

This gives hope that QEC is possible but this can only detect X errors, what if a Z error occurs?

↖ For this code we will always get syndrome $(0,0)$ and not detect an error.

The phase flip code

$$|\psi\rangle \xrightarrow{p} Z|\psi\rangle \qquad |\psi\rangle \xrightarrow{1-p} |\psi\rangle$$

← New noisy channel but with a phase flip instead of a bitflip.

Ideas?

Trick is to change viewpoint:

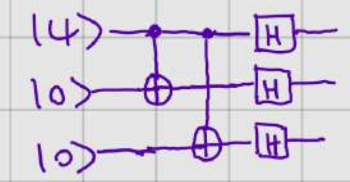
Move to Hadamard basis $|+\rangle/|-\rangle$

Z - phaseflip in $|0\rangle/|1\rangle$
X - bit flip in $|0\rangle/|1\rangle$

Z - bitflip in $|+\rangle/|-\rangle$
X - phaseflip in $|+\rangle/|-\rangle$

Then use encoding
$$|0\rangle \longmapsto |{+}{+}{+}\rangle$$
$$|1\rangle \longmapsto |{-}{-}{-}\rangle$$

Encoding map?

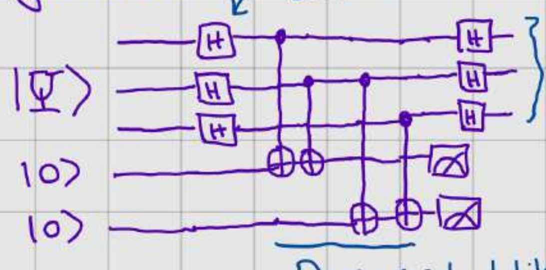


$$\alpha|0\rangle + \beta|1\rangle \longmapsto \alpha|{+}{+}{+}\rangle + \beta|{-}{-}{-}\rangle$$

$HZH = X$ So exactly like X error occured on X encoding

How to get syndrome?

Reverts corrupted state back to computational basis



converts back to $|+\rangle/|-\rangle$ basis

Does error check like in X code

The 9 qubit code (Shor)

Concatenating . phase and bitflip code

Encoding: Step 1) $|0\rangle \longmapsto |{+}{+}{+}\rangle \quad |1\rangle \longmapsto |{-}{-}{-}\rangle$

Step 2) Each qubit $|0\rangle \longmapsto |000\rangle \quad |1\rangle \longmapsto |111\rangle$

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

Overall

$$|0\rangle \longmapsto \frac{1}{2\sqrt{2}}\left(|000\rangle + |111\rangle\right)^{\otimes 3}$$

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

$$\alpha|0\rangle + \beta|1\rangle \longmapsto \frac{\alpha\left(|000\rangle + |111\rangle\right)^{\otimes 3} + \beta\left(|000\rangle - |111\rangle\right)^{\otimes 3}}{2\sqrt{2}}$$

Question: What circuit implements the 9 qubit encoding?

Syndrome detection

X errors

Same as above: check parities of

$\underbrace{(1,2),(2,3)\ \ (4,5)(5,6)\ \ (7,8)(8,9)}$

6 bits of information (6 qubits) needed to detect bitflips on the state.

Can we detect multiple errors here?

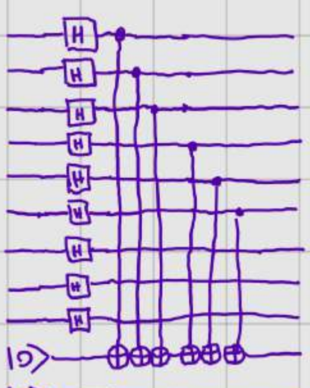
Z errors

Known as a degenerate code
Different correctable errors lead to same corrupted state.

Suppose we have a Z error on qubit $^{1,2\text{ or }3}$ then the state becomes

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

Need to compare the phases between the different partitions



$|\psi_0\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) \quad |\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle - |111\rangle\right)$

$H^{\otimes 3}|\psi_0\rangle = |000\rangle + |011\rangle + |101\rangle + |110\rangle$ ← even parity

$H^{\otimes 3}|\psi_1\rangle = |001\rangle + |010\rangle + |100\rangle + |111\rangle$ ← odd parity

Then CNOT triple gives $+1$ if $|\psi_1\rangle$
0 if $|\psi_0\rangle$

The 6 CNOTs check that the parity of input state are the same i.e. 0 if $|\psi_0\rangle|\psi_0\rangle$ or $|\psi_1\rangle|\psi_1\rangle$
1 if $|\psi_0\rangle|\psi_1\rangle$ or $|\psi_1\rangle|\psi_0\rangle$

Therefore can check phase difference between two triples!
Can correct it!

Remainder of circuit is done by checking triples 2 & 3 so can determine if a phase error occured. Can you detect multiple phase errors?
And then applying Hadamard gates recovers the original state which can be corrected depending on the syndrome observed!

<u>Remark</u>: The two detection steps are completely independent, neither affects the encoded state. Therefore we can detect and correct both an X and a Z error even if they occur on the same qubit!

We now know how to correct X and Z errors but there are an awful lot more errors to consider!

What about arbitrary errors?

Let's just give it a go...

<u>Ex</u>: $$R_\theta = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix} = \cos(\theta/2)\mathbb{1} - i\sin(\theta/2) Z$$

Suppose this error occurs on the 1st qubit in our Shor encoding $|\Psi\rangle$ (9 qubit state)

Then after error we have
$$|\Psi_E\rangle = \cos(\theta/2)|\Psi\rangle - i\sin(\tfrac{\theta}{2}) Z_1|\Psi\rangle$$

Let's put this through the syndrome detection circuit

6 qubit states

$$|\Psi_E\rangle \longmapsto \cos(\tfrac{\theta}{2})|\Psi\rangle|\text{no X error}\rangle|\text{no Z error}\rangle - i\sin(\tfrac{\theta}{2}) Z_1|\Psi\rangle|\text{no X error}\rangle|Z_1\text{ error}\rangle$$

physical qubits are now entangled with the Z error detection qubits

What happens when we measure the Z error register?

Prob	Outcome	Post Measurement state
$\cos^2(\theta/2)$	No error	$\|\Psi\rangle\|\text{no Z error}\rangle\|\text{no X error}\rangle$
$\sin^2(\theta/2)$	Z_1 error	$Z_1\|\Psi\rangle\|Z_1\text{error}\rangle\|\text{no X error}\rangle$

Magic! By measuring the syndrome we force the state to choose whether the Z part of the error occurs or not :)

Consistent with θ small being a small rotation error / coincides with small probability of Z error occuring

How does this help with arbitrary errors?

Any error E can be expressed in Pauli basis

$$E = e_0 \mathbb{1} + e_1 X + e_2 Z + e_3 \underbrace{XZ}_{Y = iXZ}$$

Extending the above example we see it can detect and correct all such errors! Shor code can correct all single qubit errors!

Remark Any QECC that can correct errors E and F can correct any linear combination $aE + bF$!

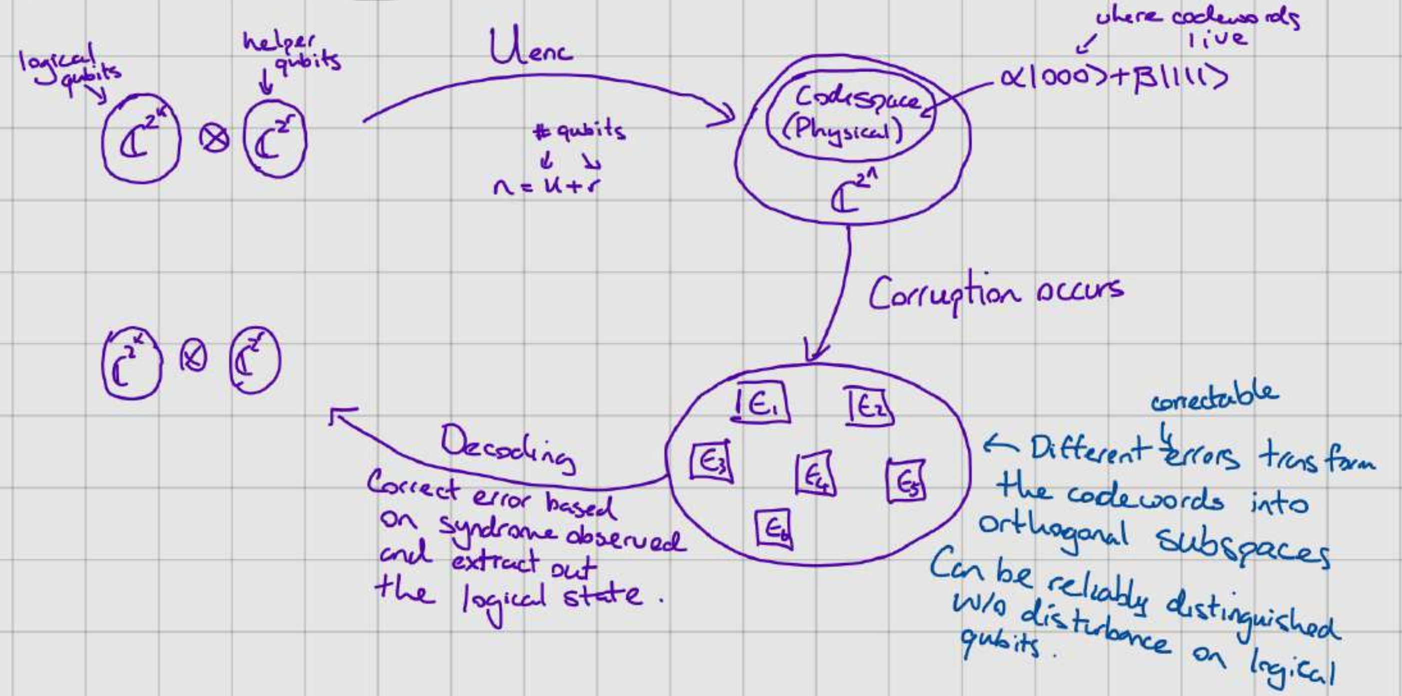
Remark (lots of small errors)

Our analysis has been under the assumption that only a single qubit gets corrupted. But as long as the errors are 'small' then we can also correct many qubit errors with a single qubit correcting code!

Let $V_\varepsilon = \mathbb{1} + \varepsilon E$ then

$$V_\varepsilon^{\otimes n} = \mathbb{1} + \varepsilon\underbrace{(E_1 + E_2 + \dots + E_n)}_{\text{all single qubit errors}} + \underbrace{O(\varepsilon^2)}_{\text{negligible for small enough } \varepsilon.}$$

General Quantum Codes (binary)



A quantum code is then defined by this procedure, i.e., an encoding / syndrome detection / decoding procedure and the set of correctable errors $\mathcal{E}$.

↖ For Shor code this includes all single qubit errors.

What are some necessary and sufficient conditions to correct errors in $\mathcal{E}$?

Let $\{|\bar{i}\rangle\}$ denote an orthonormal basis of the codespace.

It is necessary that

$$\langle \bar{j} | E_b^\dagger E_a | \bar{i} \rangle = 0 \qquad i \neq j$$

If this was not the case then $E_a|\bar{i}\rangle$ and $E_b|\bar{j}\rangle$ would not be perfectly distinguishable despite $\langle \bar{j} | \bar{i} \rangle = 0$. (Perfectly distinguishable $\Leftrightarrow$ orthogonal)

A sufficient condition is that

non degenerate

$$\langle \bar{j} | E_a^\dagger E_b | \bar{i} \rangle = \delta_{ab}\delta_{ij}$$

In this case we can always distinguish different errors and so we can measure the projectors onto the subspaces and correct like in the Shor code.

It turns out that a necessary and sufficient condition for recovery is that

$$\langle \bar{j} | E_b^\dagger E_a | \bar{i} \rangle = C_{ba} \delta_{ij}$$

where $C_{ba} = \langle \bar{i} | E_b^\dagger E_a | \bar{i} \rangle$ (does not depend on $|\bar{i}\rangle$) is a Hermitian matrix.

Proof: See Nielsen & Chuang

Example: Consider the X code

A basis for the codespace was $|000\rangle$ $|111\rangle$

$\mathcal{E} = \{X_1, X_2, X_3, \mathbb{1}\}$

$$\langle 000 | X_i X_j | 111 \rangle \overset{\forall ij}{=} 0 \qquad \left.\begin{array}{l}\langle 000 | X_i X_j | 000 \rangle \\ \langle 111 | X_i X_j | 111 \rangle\end{array}\right\} = \delta_{ij}$$

$$C_{ab} = \begin{array}{c} \\ X_a \end{array}\begin{array}{c|cccc} & \multicolumn{4}{c}{X_b} \\ & 1 & X_1 & X_2 & X_3 \\ \hline 1 & 1 & 0 & 0 & 0 \\ X_1 & 0 & 1 & 0 & 0 \\ X_2 & 0 & 0 & 1 & 0 \\ X_3 & 0 & 0 & 0 & 1 \end{array}$$

What breaks if we add Z_1? (C_{ab} suddenly depends on $|\bar{i}\rangle$)

Distance of a code

We only care about Pauli errors as by the argument before these will allow us to correct other errors.

We consider tensor products of Pauli operators $\{\mathbb{1}, X, Y, Z\}$ of n-qubit systems. $X \otimes \mathbb{1} \otimes X \otimes \ldots \equiv X_1 X_3 \ldots$

The *weight* of an operator from this set is the number of non-identity Pauli operators in the tensor product.

Ex: $X_1 X_5$ has weight 2 $\qquad Z_1 Z_2 X_4 Y_5$ has weight 4

Def^n (Distance)

The distance of a code is the minimal weight Pauli operator such that $\langle \bar{i} | E_a | \bar{j} \rangle \neq C_a \delta_{ij}$

Ex: For the X code the distance is 1. (C_a is dependent on $|\bar{i}\rangle$ if we use Z)

Note that if we want to be able to correct <u>all</u> Pauli operators of weight t. Then we need a distance $d \geq 2t+1$

If $d \leq 2t$ then

$$\langle \bar{i} | (\underbrace{E_b^\dagger E_a}_{\text{weight } 2t}) | \bar{j} \rangle \neq C_{ab}\, \delta_{ij}$$

for weight t E_a, E_b which are by assumption correctable.

<u>Remark (Degenerate code)</u>

We call a code degenerate if two different errors $E_a \neq E_b$ can act the same way on the codespace i.e. $E_a|\psi\rangle = E_b|\psi\rangle$ $\forall\ |\psi\rangle$ in the codespace.

Ex: The Shor code is degenerate. Consider how a Z error acts on different qubits in a block.

Degeneracy is <u>not</u> a feature of classical ECCs, there different errors will always have different effects. It gives us hope to find more efficient methods to correct errors as it implies that different errors may be treated as the same.

Notation $[[n,k,d]]$ code has k logical qubits
n physical qubits
distance d.

What's the best we can hope for? (Quantum Hamming bound)

Suppose we have a non-degenerate $[[n,k,d]]$ code for some given k and d, what constraints on n do we have?

On a given qubit we have 3 possible Pauli errors. So the total number of errors on t or fewer qubits is

$$\sum_{j=0}^{t} \binom{n}{j} 3^j$$

← 0 term denotes no error

Each error must correspond to a k-qubit subspace as we're non-degenerate. So in total we need a space at least as big as

$$\boxed{2^k \sum_{j=0}^{t} \binom{n}{j} 3^j \leq 2^n}$$

Quantum Hamming bound

For $t=1$ (single qubit errors) we get $2(1+3n) \leq 2^n \Rightarrow n \geq 5$

This suggests we can do better than Shor and indeed we can!

NB: Examples of degenerate codes that beat the Hamming bound are known!

The Stabilizer Formalism

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Def^n (Pauli group)

The Pauli group on n qubits (P_n) is defined as the group consisting of all tensor products of $\{\mathbb{1}, X, Y, Z\}$ with overall phases $\{\pm 1, \pm i\}$

Needed to ensure group structure. $Y = iXZ$

Example $iZ \otimes X \otimes \mathbb{1} \in P_3$ ← denote this iZ_1X_2

Properties

1) $|P_n| = 4^{n+1}$ 4^n tensor products $\times$ 4 phases

2) $P \in P_n \implies$ eigenvalues $\in \{\pm 1, \pm i\}$ All Pauli operators have eigs ± 1. Tensor products give products of eigenvalues

3) $\forall M, N \in P_n$ either $MN = NM$ or $MN = -NM$
   All Paulis either commute or anticommute.

4) $M \in P_n \implies M^2 = \pm \mathbb{1}$ $\mathbb{1} = \mathbb{1}^2 = X^2 = Y^2 = Z^2$

Alternative viewpoint on Shor Code

Recall $\alpha(|000\rangle + |111\rangle)^{\otimes 3} + \beta(|000\rangle - |111\rangle)^{\otimes 3} \equiv |\Psi\rangle$

Note $|00\rangle$ $|11\rangle$ are eigenvectors of Z_1Z_2 with eigenvalue $+1$
$|01\rangle$ $|10\rangle$ " " with eigenvalue -1

Thus measuring Z_1Z_2 on $|\Psi\rangle$ will conduct a parity check on first two qubits w/o disturbing state

We can think of the bitflip checks as performing the measurements

M_1 Z_1Z_2
M_2 Z_2Z_3
M_3 Z_4Z_5
M_4 Z_5Z_6
M_5 Z_7Z_8
M_6 Z_8Z_9

Requires 6 2qubit measurements
6 bits of information

Doesn't disturb state as all codewords are eigenvectors.

How about phase errors?

$|000\rangle + |111\rangle$ is $+1$ eigenvector of $X \otimes X \otimes X$
$|000\rangle - |111\rangle$ is -1 eigenvector of $X \otimes X \otimes X$

So if we measure $X_1X_2X_3X_4X_5X_6$ $\begin{cases} \xrightarrow{+1} \text{Phases are the same} \\ \xrightarrow{-1} \text{Phases are different} \end{cases}$

And again no disturbance as codewords (even corrupted) are eigenvectors!

M_7 $X_1X_2X_3X_4X_5X_6$
M_8 $X_4X_5X_6X_7X_8X_9$

2 bits of information for phase error (block check)

Measurement choices are not unique. E.g. could use X_1X_3, however $X_1X_3 = (X_1X_2)(X_2X_3)$ so its value can be determined by X_1X_2 and X_2X_3 (product of eigenvalues). Everything here commutes, may be worth considering the group generated by these operators.

<u>Def^n (Stabilizer)</u>

Let T be a subspace of $(\mathbb{C}^2)^{\otimes n}$. The <u>stabilizer</u> of T is

$$S(T) = \{ P \in P_n : \underset{\leftarrow +1 \text{ eigenstate}}{P|\psi\rangle = |\psi\rangle} \quad \forall\ |\psi\rangle \in T \}$$

Example Shor code has codespace $V = \text{span}\{(|000\rangle+|111\rangle)^{\otimes 3}, (|000\rangle-|111\rangle)^{\otimes 3}\}$

Can check $Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9$

$X_1X_2X_3\ldots X_6$, $X_4X_5\ldots X_9$ are all in the stabilizer of V.

In fact the full stabilizer is the group generated by the above operators.

Properties of Stabilizer

1) $-I \notin S(T)$ everything is -1 eigenvector

2) $S(T)$ forms a group subgroup of P_n by def^n easy to check

3) $S(T)$ is an Abelian group $MN = NM$

If $MN = -NM$ then $|\psi\rangle = MN|\psi\rangle = -NM|\psi\rangle = -|\psi\rangle$ contradiction

4) Given r minimal generators then $|S| = 2^r$

They commute so can take them as bit strings

Ex: Shor code $|S| = 2^8$

Idea: Stabilizers allow us to construct new codes from the set of operators

Start with $S \subseteq P_n$ an Abelian subgroup s.t. $-I \notin S$

Then define

$$T(S) := \{|\psi\rangle : M|\psi\rangle = |\psi\rangle \ \forall M \in S\}$$

Simultaneous +1 eigenspace.

How big is $T(S)$?

Lemma Let S be an Abelian subgroup of P_n and $-I \notin S$. Then the dimension of $T(S)$ is 2^{n-r} where r is the number of generators of S.

<u>Proof</u> Intuitively each generator chops the Hilbert space in 2 parts, Halving the +1 eigenspace each time.

Formally, define projector onto codespace

$$\Pi_{T(S)} = \frac{1}{2^r} \sum_{M \in S} M$$

Why is this the projector? Well $\forall\ |\psi\rangle \in T(S)$ we have

$$\Pi_{T(S)} |\psi\rangle = \frac{1}{2^r} \sum_{M \in S} M |\psi\rangle = \frac{1}{2^r} \sum_{M \in S} |\psi\rangle = |\psi\rangle$$

Moreover, $\forall |\psi\rangle \in H$ we want $\Pi_{T(S)} |\psi\rangle \in T(S)$. Take $N \in S$ then

$$N(\Pi_{T(S)} |\psi\rangle) = \frac{1}{2^r} \sum_{M \in S} NM |\psi\rangle = \frac{1}{2^r} \sum_{M \in S} M |\psi\rangle = \Pi_{T(S)} |\psi\rangle$$

as N was arbitrary we must have $\Pi_{T(S)} |\psi\rangle \in T(S)$.

Now we have a projector, so the dimension of the subspace is

$$\mathrm{Tr}(\Pi_{T(S)}) = \frac{1}{2^r} \sum_{M \in S} \mathrm{Tr}(M) = \frac{1}{2^r} \mathrm{Tr}(\mathbb{1}^{\otimes n}) = 2^{n-r}$$ ☒

Stabilizers can help detect errors

Suppose we have an error $E \in P_n$ such that $\{E, M\} = 0$ for some $M \in S$.

$$\text{Let } |\psi\rangle \in T(S) \xrightarrow{\text{Error}} E|\psi\rangle$$

is $E|\psi\rangle$ still a codeword?

$$\text{Well } ME|\psi\rangle = -EM|\psi\rangle = -E|\psi\rangle$$

$E|\psi\rangle$ is -1 eigenvector of M!

So measuring M detects that some error occurred. and no disturbance

- Only other case is that $[E, M] = 0$ but here we have

$$ME|\psi\rangle = EM|\psi\rangle = E|\psi\rangle$$

so $E|\psi\rangle \in T(S)$ and is undetectable!

Let

$$N(S) := \{ M \in P_n : [M,N] = 0 \ \forall N \in S \}$$

Then the set of undetectable errors is $N(S) \setminus S$

← why $\setminus S$?

+1 outcome $\xrightarrow{\text{think}}$ no error occured

but if $E \in S$ then $E|\psi\rangle = |\psi\rangle$ so 'error' acts trivially!

Stabilizers can correct errors

Why can we do this?

Measure each of the generators of S to construct the error syndrome

$$\begin{array}{c} M_1 \\ M_2 \\ \vdots \end{array} \begin{pmatrix} +1 \\ +1 \\ -1 \\ +1 \\ \vdots \end{pmatrix}$$

Error E must anticommute with generator M_3

Why do we need to only measure the generators?

Lemma Suppose one of the following holds

1) $E_b^\dagger E_a \in S$
2) $\exists\ M \in S$ such that $\{M, E_b^\dagger E_a\} = 0$

Then $E_a, E_b \in \mathcal{E}$.

Proof We want to show the sufficient condition

$$\langle \psi | E_b^\dagger E_a | \psi \rangle = C_{ab} \qquad \forall\, a,b \text{ and } |\psi\rangle \in T(S)$$

degenerate code.

In case 1) then $\langle \psi | E_b^\dagger E_a | \psi \rangle = \langle \psi | \psi \rangle = 1$ ✓

In case 2) then suppose $M \in S$ such that $\{M, E_b^\dagger E_a\} = 0$

Then $\langle \psi | E_b^\dagger E_a | \psi \rangle = \langle \psi | E_b^\dagger E_a M | \psi \rangle = -\langle \psi | M E_b^\dagger E_a | \psi \rangle$

$= -\langle\psi|E_b^\dagger E_a|\psi\rangle \quad \Rightarrow \quad \langle\psi|E_b^\dagger E_a|\psi\rangle = 0$ ✓ $\boxtimes$

Suppose E_a and E_b are two Pauli errors with the same error syndrome

$\Rightarrow$ E_a and E_b must commute with the same $M \in S$

$\Rightarrow$ $[E_a^\dagger E_b, M] = 0 \quad \forall M \in S$

$\Rightarrow$ $E_a^\dagger E_b \in N(S)$

$$\boxed{\text{A stabilizer code } S \text{ can correct } \mathcal{E} \subseteq P_n \iff E_a^\dagger E_b \notin N(S)\setminus S.}$$

A better code [[5,1,3]]

We consider the following code for $n=5, k=1$

$M_1 = X\,Z\,Z\,X\,\mathbb{1}$
$M_2 = \mathbb{1}\,X\,Z\,Z\,X$
$M_3 = X\,\mathbb{1}\,X\,Z\,Z$
$M_4 = Z\,X\,\mathbb{1}\,X\,Z$

Can check this gives an Abelian subgroup of P_5

Can also check that the code has distance 3 as every weight 1 and weight 2 Pauli operator anti commutes with at least one generator.

$\Rightarrow$ it should correct all 1 qubit errors.

Indeed there are 4 bits of information here and $3\times 5 + 1 = 16$ possible error states.

$\Rightarrow$ Perfect non-degenerate code for single qubit error detection.

CSS codes (Stabilizer codes from ECCs)

Recall a classical binary linear code is defined by a generator matrix $G \in \mathbb{M}_{k\times n}(\mathbb{F}_2)$.
Given logical bitstring v we get a codeword $G^T v$.
distance: minimal Hamming distance between two codewords

We also have a parity check matrix H which produces the error syndrome $\quad Hw$

← matrix of maximal rank such that $HG^T = 0$

Ex: Hamming [7,4,3] code

$$H = \begin{pmatrix} 1111000 \\ 1100110 \\ 1010101 \end{pmatrix}$$

Connection to stabilizers

Take two classical codes C_1 and C_2 replace
For C_1 replace parity matrix with Z operators
For C_2 replace parity matrix with X operators

Ex

$$\left.\begin{matrix} ZZZZ111 \\ ZZ11ZZ1 \\ Z1Z1Z1Z \end{matrix}\right\}[7,4,3] \qquad \longrightarrow [[7,1,3]]\ \text{QEC}$$

$$\left.\begin{matrix} XXXX111 \\ XX11XX1 \\ X1X1X1X \end{matrix}\right\}[7,4,3]$$

* Systematic method to construct quantum codes from classical codes.

* Doesn't always work: need to check that resulting group is Abelian.
Abelian $\iff v\cdot w = 0 \ \forall v,w$ where v row in H_1 and w row in H_2

H_i parity check matrix for code C_i.

Quantum Channels

What is the most general evolution of a quantum system?

$$\underset{\mathcal{H}_1}{\rho} \xrightarrow{\mathcal{E}} \underset{}{\overset{H_2}{\sigma}} = \mathcal{E}(\rho)$$

ρ, σ quantum states

Requirements?

* Linear $\quad p\rho_1 + (1-p)\rho_2 \longmapsto p\,\mathcal{E}(\rho_1) + (1-p)\,\mathcal{E}(\rho_2)$

* Trace preserving: $\mathrm{Tr}[\rho] = \mathrm{Tr}[\mathcal{E}(\rho)]$

* Completely positive: $(\mathcal{E}_A \otimes I_B)(\rho_{AB}) \geq 0 \quad \forall$ systems B.

  If we apply it to a subsystem then the joint system after should still be PSD

Def^n (Quantum Channel)

A quantum channel from $\mathcal{H}_A$ to $\mathcal{H}_B$ is a linear map $\mathcal{E}: \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ that is trace preserving and completely positive (CPTP map)

Example

* $\mathcal{E}(\rho) = U\rho U^\dagger$ for some unitary U

Interpretation?

(Replacement) * $\mathcal{E}(\rho) = \mathrm{Tr}[\rho]\,\sigma$ for some quantum state σ.

(depolarizing) • $\mathcal{E}(\rho) = \gamma\rho + (1-\gamma)\,\mathrm{Tr}(\rho)\,\mathbb{1}/d$ $\quad$ dimension $\quad \gamma \in [0,1]$

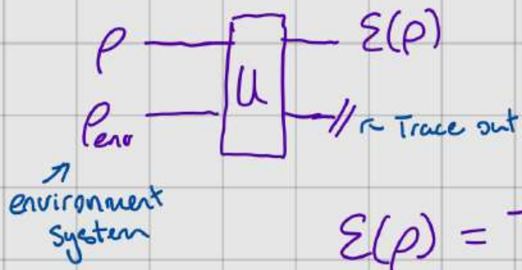
(dephasing) • $\mathcal{E}(\rho) = \gamma\rho + (1-\gamma)\,Z\rho Z$ $\quad$ (qubit channel)

• $\mathcal{E}(\rho) = \mathrm{Tr}(\rho)$ or $\mathcal{E}(\rho) = \mathrm{Tr}_A[\rho]$

What feature do we lose with general quantum channels? (Reversibility).

Open vs. Closed systems

Recall for closed systems the dynamics are unitary



$$\mathcal{E}(\rho) = \mathrm{Tr}_{env}\left[U(\rho \otimes \rho_{env})U^{\dagger}\right]$$

A result known as <u>Stinespring dilation</u> says that any channel can be written in this way. Non-unitarity corresponds to some information loss to the environment. If we include the environment we can recover unitarity.

<u>Kraus Representation</u> Let $\{|e_k\rangle\}_k$ be an ONB for the environment, then
orthonormal basis

$$\mathcal{E}(\rho) = \sum_k \langle e_k| U(\rho \otimes |e_0\rangle\langle e_0|)U^{\dagger}|e_k\rangle$$

$$= \sum_k E_k \rho E_k^{\dagger} \quad \text{where} \quad E_k = (\mathbb{1} \otimes \langle e_k|)\,U\,(\mathbb{1} \otimes |e_0\rangle)$$

$$\equiv \langle e_k| U |e_0\rangle$$

Shorthand $|e_i\rangle = \mathbb{1} \otimes |e_i\rangle$

These operators satisfy a completeness relation

$$\sum_k E_k^{\dagger} E_k = \sum_k \langle e_0| U |e_k\rangle\langle e_k| U^{\dagger} |e_0\rangle$$

$$= \langle e_0| U U^{\dagger} |e_0\rangle$$

$$= \langle e_0|e_0\rangle = \mathbb{1}$$

$$\sum_k E_k^{\dagger} E_k = \mathbb{1}$$

Let $\{A_k\}_k$ be a set of linear operators ($A_k \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$) such that $\sum_k A_k^{\dagger} A_k = \mathbb{1}_A$

Then $\mathcal{E}(\rho) = \sum_k A_k \rho A_k^{\dagger}$ is a quantum channel

Known as Kraus representation
$\{A_k\}$ – Kraus operators.

By the above all channels have this Kraus sum representation.

<u>Proof</u>: Exercise.

Choi matrix isomorphism (Bonus)

Suppose we have a channel $\mathcal{E}: \mathcal{L}(A) \to \mathcal{L}(A)$. Consider the non-normalized vector $|\Phi\rangle = \sum_i |i\rangle_A |i\rangle_R$ where R is a system of same dimension as A.

Consider the map

Choi matrix of $\mathcal{E}$

$$\begin{aligned} J(\mathcal{E}) &= (\mathcal{E} \otimes I)(|\Phi\rangle\langle\Phi|) \\ &= (\mathcal{E} \otimes I)\Big(\sum_{ij} |ii\rangle\langle jj|\Big) \\ &= \sum_{ij} \mathcal{E}(|i\rangle\langle j|) \otimes |i\rangle\langle j| \end{aligned}$$

$J(\mathcal{E})$ is now a matrix acting on AR.

One can show this map defines a linear bijection between the set of channels $\mathcal{E}: \mathcal{L}(A) \to \mathcal{L}(A)$ and the set of positive semidefinite operators on AR

Choi-Jamiołkowski isomorphism

$$\Phi(X) = \mathrm{Tr}_R\big(J(\mathcal{E})(\mathbb{1}_A \otimes X^T)\big)$$ inverse mapping

Map is completely positive $\iff$ Choi matrix is positive semidefinite

Map is trace preserving $\iff$ $\mathrm{Tr}_A[J(\mathcal{E})] = \mathbb{1}_R$

Can also derive Kraus operators from the eigenvectors of $J(\mathcal{E})$ and the map $|i\rangle|j\rangle \longmapsto |i\rangle\langle j|$.