Quantum Error Correction

See
errorcorrectionzoo.org

We know classically that error correction is an important concept:

data $x \xrightarrow{\text{errors}} y$ corrupted data

error correction

data $\xrightarrow{\text{encode}}$ codeword $\downarrow$ corrupted codeword $\xrightarrow{\text{correction}}$ codeword $\xrightarrow{\text{decoding}}$ data

Useful for lossy communication / computation / storage.

The simplest code

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

Noisy Channel

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

$x \xrightarrow{1-p} x$

Suppose p is small

(with prob p we have a bitflip)

Probability p of error.

Idea: Add redundancy...

We encode our bit x into a codeword

$0 \longmapsto 000$

$1 \longmapsto 111$

Use 3 bits to encode 1 logical bit

Assume channel acts in IID way

$x=0$ (similar for $x=1$)

Output	Probability
000	$(1-p)^3$
001	$p(1-p)^2$
010	$p(1-p)^2$
100	$p(1-p)^2$
⋮	$O(p^2)$

Use majority voting

000, 001, 010, 100 $\longmapsto 0$

111, 110, 101, 011 $\longmapsto 1$

Probability of error is now $\varepsilon_{rep} = p^3 + 3p^2(1-p)$

Old probability of error was $\varepsilon = p$

Notice $\varepsilon_{rep} < \varepsilon$ whenever $p < \frac{1}{2}$.

advantage for repetition code.

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

A first attempt at QEC

Quantum systems <u>need</u> error correction.

Maybe we can replicate classical EC

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

We then measure for errors and take majority vote...

However there are serious problems with this scheme (What can you think of?)

1) No cloning: if $|\psi\rangle$ is unknown we cannot reliably make copies.

2) Error detection: measuring disturbs the system

3) Many errors: we no longer just have bit-flip errors

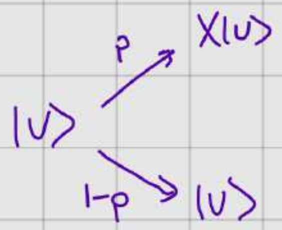
Z, Y, U ← continuum of errors.

It seems hopeless but we can deal with all these difficulties!

The bitflip code

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

Let's make the problem easier and consider only X errors

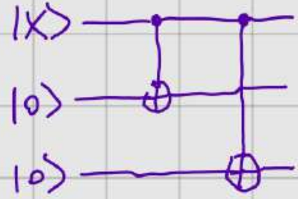


We make following encoding

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

Why does this not violate no-cloning?

This can be done with a circuit



So we start with qubit $|\chi\rangle = \alpha|0\rangle + \beta|1\rangle$ and it becomes codeword $|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$

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

Now pass each qubit through the channel

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

What can we do now?

With high probability we get one of those 4 states. But they all live in different orthogonal subspaces and so can be reliably distinguished

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111| \qquad \text{(no error)}$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011| \qquad \text{(Qubit 1 error)}$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

These measurements will not disturb the state and perfectly distinguish

Ex:

$$\langle\psi|P_i|\psi\rangle = \delta_{i0}$$
$$\langle\psi|(X\otimes\mathbb{1}\otimes\mathbb{1})\, P_i\, (X\otimes\mathbb{1}\otimes\mathbb{1})|\psi\rangle = \delta_{i1}$$
$$\vdots$$

So we detect the error without disturbing the state and then we can correct it!

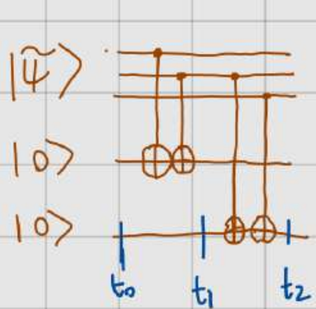
apply X to appropriate qubit.

A circuit viewpoint on error detection

$X_j = \mathbb{1}\otimes\ldots\mathbb{1}\otimes X\otimes\mathbb{1}\otimes\ldots\otimes\mathbb{1}$ (qubit j)

With high probability we have a state $|\tilde{\psi}\rangle \in \{|\psi\rangle, X_1|\psi\rangle, X_2|\psi\rangle, X_3|\psi\rangle\}$

Idea: check pairwise parities between the qubits



t_0: $(\alpha|abc\rangle + \beta|\bar{a}\bar{b}\bar{c}\rangle)|0\rangle|0\rangle$

t_1: $\alpha|abc\rangle|a\oplus b\rangle|0\rangle + \beta|\bar{a}\bar{b}\bar{c}\rangle|\bar{a}\oplus\bar{b}\rangle|0\rangle$

t_2: $\alpha|abc\rangle|a\oplus b\rangle|b\oplus c\rangle + \beta|\bar{a}\bar{b}\bar{c}\rangle|\bar{a}\oplus\bar{b}\rangle|\bar{b}\oplus\bar{c}\rangle$

Note $x \oplus y = \bar{x} \oplus \bar{y}$ so the final state is

Important as implies measurement qubits 4 and 5 will not affect qubits 1, 2 and 3.

$$\underbrace{(\alpha|abc\rangle + \beta|\bar{a}\bar{b}\bar{c}\rangle)|a\oplus b\rangle|b\oplus c\rangle}$$

not entangled

Qubits 4 and 5 now encode parity checks we measure in $\{|0\rangle, |1\rangle\}$ basis we find

Measurement result	Conclusion	
00	no error	$\mathbb{1}$
01	qubit 3 error	X_3
10	qubit 1 error	X_1
11	qubit 2 error	X_2

error syndrome

This gives hope for QEC. But what about other errors?

Suppose Z error occurs instead $\quad |\psi\rangle \longmapsto \alpha|000\rangle - \beta|111\rangle$

Error detection step says 'no error' always!

Applying the code actually makes Z errors worse because we increase the number of qubits that they can occur on...

The phase flip code

$$|\psi\rangle \begin{cases} \xrightarrow{p} Z|\psi\rangle \\ \xrightarrow{1-p} |\psi\rangle \end{cases}$$

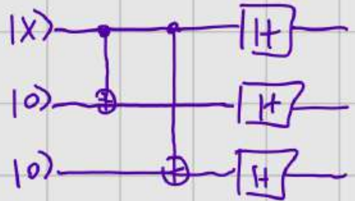
Now we consider 'phase flip' errors.

Idea: Change viewpoint. $\quad Z|+\rangle = |-\rangle \quad Z|-\rangle = |+\rangle$

Z acts like an X error when applied to $\{|+\rangle, |-\rangle\}$ basis.

So we use an encoding $|0\rangle \longmapsto |+\rangle|+\rangle|+\rangle$

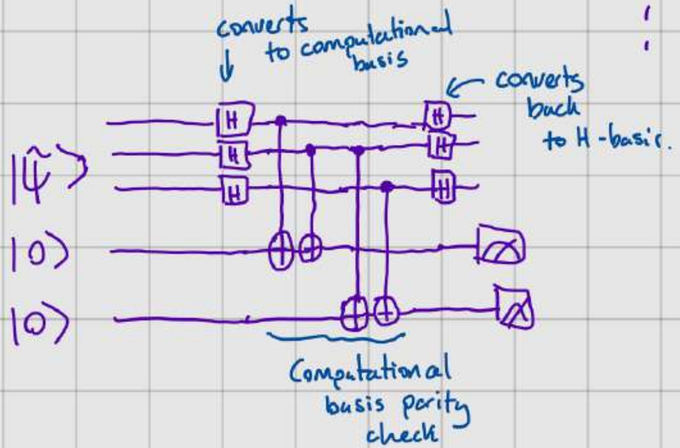
$|1\rangle \longmapsto |-\rangle|-\rangle|-\rangle$



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

prob	$\vert\tilde{\psi}\rangle$
$(1-p)^3$	$\alpha\vert{+}{+}{+}\rangle + \beta\vert{-}{-}{-}\rangle$
$p(1-p)^2$	$\alpha\vert{-}{+}{+}\rangle + \beta\vert{+}{-}{-}\rangle$
$\vdots$	$\alpha\vert{+}{-}{+}\rangle + \beta\vert{-}{+}{-}\rangle$
$\vdots$	$\alpha\vert{+}{+}{-}\rangle + \beta\vert{-}{-}{+}\rangle$

How to get syndrome?



Can read out which qubit had Z error and can correct it!

By symmetry this code will make X errors worse!

The 9 qubit code (Shor)

We want to correct X and Z simultaneously. To do so we try concatenation of the above codes.

Encoding: Step 1) $|0\rangle \longmapsto |{+}{+}{+}\rangle$ $\quad |1\rangle \longmapsto |{-}{-}{-}\rangle$ $\quad (1 \mapsto 3$ qubits$)$

Step 2) $|0\rangle \longmapsto |000\rangle$ $\quad |1\rangle \longmapsto |111\rangle$ $\quad (3 \mapsto 9$ qubits$)$

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

So encoded state is $|\psi\rangle = \frac{\alpha}{2\sqrt{2}}\left(|000\rangle + |111\rangle\right)^{\otimes 3} + \frac{\beta}{2\sqrt{2}}\left(|000\rangle - |111\rangle\right)^{\otimes 3}$.

Errors

X errors Imagine we check parities of $\overbrace{(1,2),(2,3),\ (4,5),(5,6),\ (7,8),(8,9)}^{6 \text{ bits of information}}$.

For no error the parities will be 000000

Error	Parity string
$\mathbb{1}$	000000
X_1	100000
X_2	110000
X_3	010000
X_4	001000
$\vdots$	$\vdots$

Can see on which qubit the error occured.

Can we detect multiple X errors here?

Z errors

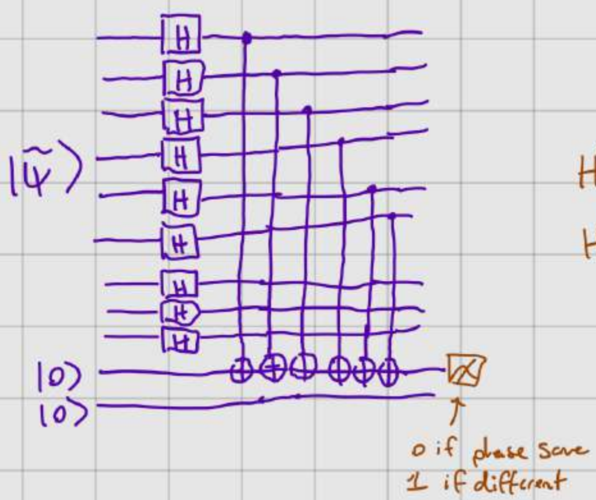
Suppose a Z error occurs on qubit 1,2 or 3. then the state becomes

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

Error on 1,2 or 3 leads to same state. Known as a degenerate code.

Idea: Check phase parity between blocks

Checking phase parity between block 1 and 2.



$$|\psi_0\rangle = \frac{|000\rangle+|111\rangle}{\sqrt{2}} \qquad |\psi_1\rangle = \frac{|000\rangle-|111\rangle}{\sqrt{2}}$$

$$H^{\otimes 3}|\psi_0\rangle = \frac{|000\rangle+|011\rangle+|101\rangle+|110\rangle}{2}$$ even parity

$$H^{\otimes 3}|\psi_1\rangle = \frac{|001\rangle+|010\rangle+|100\rangle+|111\rangle}{2}$$ odd parity

So the check to the left gives

0 for $|\psi_0\rangle|\psi_0\rangle$ or $|\psi_1\rangle|\psi_1\rangle$

1 for $|\psi_0\rangle|\psi_1\rangle$ or $|\psi_1\rangle|\psi_0\rangle$

Therefore we can detect the phase difference between the triples and correct it!

Can you detect multiple phase errors?

Remark

The two detection and correction steps are completely independent. Correcting an X error does not affect the Z error (and vice-versa).

Therefore we can simultaneously detect and correct both errors even if they are on the same qubit!

What about arbitrary errors?

Let's just blindly try...

Consider $R_\theta = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix} = \cos(\frac{\theta}{2})\mathbb{1} - i\sin(\frac{\theta}{2})Z$

Suppose this error occurs on the 1st qubit of the shor encoded state $|\psi\rangle$

After error we have

$$|\tilde{\psi}\rangle = \cos\left(\frac{\theta}{2}\right)|\psi\rangle - i\sin\left(\frac{\theta}{2}\right)Z_1|\psi\rangle$$

Let's put it through the syndrome detection circuit, we get

$$\cos\left(\frac{\theta}{2}\right)\underbrace{|\psi\rangle}_{9\text{ qubits}}\underbrace{|\text{no } Z \text{ error}\rangle}_{2\text{ qubits}}\underbrace{|\text{no } X \text{ error}\rangle}_{6\text{ qubits}} - i\sin\left(\frac{\theta}{2}\right)Z_1|\psi\rangle|Z_1\text{ error}\rangle|\text{no } X\text{ error}\rangle$$

$$= \left(\cos\left(\frac{\theta}{2}\right)|\psi\rangle|\text{no } Z\text{ error}\rangle - i\sin\left(\frac{\theta}{2}\right)Z_1|\psi\rangle|Z_1\text{ error}\rangle\right)|\text{no } X\text{ error}\rangle$$

code state now becomes entangled with Z error detection register

What happens if we measure Z syndrome?

Prob	Conclusion	Post-measurement state
$\cos(\frac{\theta}{2})^2$	no error	$\|\psi\rangle\|\text{no } Z\text{ error}\rangle\|\text{no } X\text{ error}\rangle$
$\sin(\frac{\theta}{2})^2$	Z_1 error	$Z_1\|\psi\rangle\|Z_1\text{ error}\rangle\|\text{no } X\text{ error}\rangle$

Magic! By measuring the syndrome we force the system to 'choose' which error occurs. Now the post-measurement state is correctable.

When θ is close to 0 the probability of observing an error is small. Consistent with $R_\theta \approx \mathbb{1}$ when $\theta \approx 0$.

Arbitrary single qubit unitaries

Any error E can be expressed in the Pauli basis as

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

$Y = iXZ$ so we can correct it!

Extending the above example shows that the shor code can correct any single qubit unitary error!

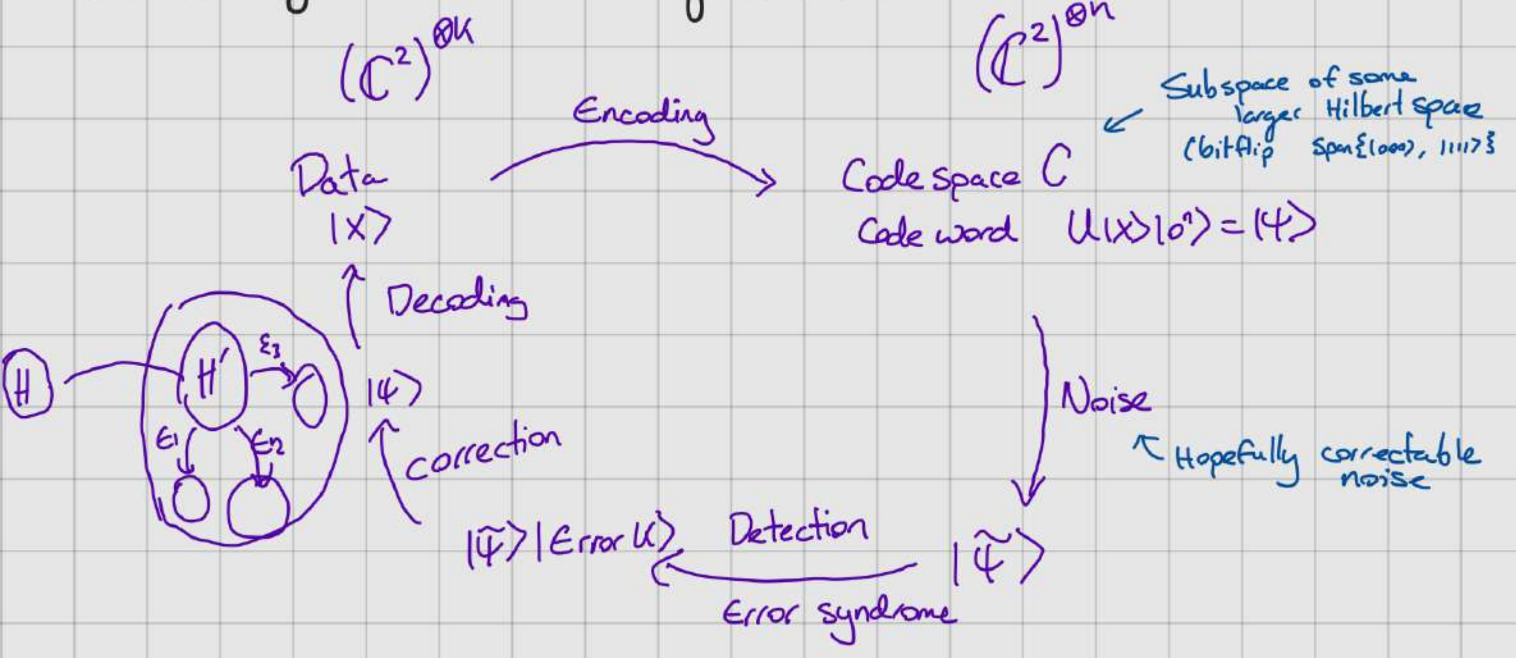
Remark (Many small errors)

So far we have assumed that only a single qubit gets corrupted. This is far from reality and very likely all qubits will receive some small error. But as long as they are small we should still be ok with the above code. Let $V_\varepsilon = \mathbb{1} + \varepsilon E$ (error close to $\mathbb{1}$) then

$$V_\varepsilon^{\otimes n} = \mathbb{1} + \varepsilon(E_1 + E_2 + \ldots + E_n) + O(\varepsilon^2)$$

all single qubit errors which we can correct linear combinations of!

A more general framework for QEC



Intuition: Different errors map orthogonal codewords to different orthogonal Subspaces (distinguishable).

However for any QECC you will have errors that cannot be corrected!

Eg. - Phase flips in the bitflip code

- $X_1 X_2$ error in the Shor code (two qubit error on same block).

Fortunately given a codespace C we can characterize exactly the set of correctable errors $\mathcal{E}$.

Note: We only consider unitary errors here but more general errors exist using the framework of quantum channels.

Th^m (Knill-Laflamme)

Let $\mathcal{E}$ be some linear space of errors acting on a Hibert space $\mathcal{H}$.
Let $H_c \subseteq \mathcal{H}$ be a codespace, then this QECC can correct all errors in $\mathcal{E}$ iff $\exists$ a Hermitian matrix C_{ab} such that

$$\langle \psi_i | E_a^\dagger E_b | \psi_j \rangle = C_{ab}\, \delta_{ij}$$

for all $E_a, E_b \in \mathcal{E}$ and $\{|\psi_i\rangle\}_i$ form an orthonormal basis for H_c.

sufficient to check a basis.

Proof is beyond the scope of the lecture but we can still see some intuition in the conditions:

- the δ_{ij} tells us that correctable errors should keep orthogonal states orthogonal. States are perfectly distinguishable $\Leftrightarrow$ they are orthogonal. So if $\langle \psi_i | E_a^\dagger E_b | \psi_j \rangle \neq 0$ when $i \neq j$ then we cannot have a procedure that maps them back to $|\psi_i\rangle$ $|\psi_j\rangle$. Otherwise we would have a procedure to distinguish non-orthogonal states.

- Secondly we want $\langle \psi_i | E_a^\dagger E_b | \psi_i \rangle = \langle \psi_j | E_a^\dagger E_b | \psi_j \rangle$. If this was not true then probability of distinguishing $E_a|\psi_i\rangle$ and $E_b|\psi_i\rangle$ would depend on the basis state $|\psi_i\rangle$. Problem for superpositions.
  Suppose $\langle \psi_0 | E_a^\dagger E_b | \psi_0 \rangle = c_0$ $\langle \psi_1 | E_a^\dagger E_b | \psi_1 \rangle = c_1$ consider $|\psi\rangle = \frac{\frac{1}{\sqrt{c_0}}|\psi_0\rangle + \frac{1}{\sqrt{c_1}}|\psi_1\rangle}{N}$
  $|\psi^\perp\rangle = \frac{\frac{1}{\sqrt{c_1}}|\psi_0\rangle - \frac{1}{\sqrt{c_0}}|\psi_1\rangle}{N}$

If we have a code that maps k qubits to n qubits and can correct all errors on t or fewer qubits then we say it is a

$$[[n, k, 2t+1]] \text{ code}$$

distance: minimum # of qubit errors needed to move from one codeword to another

Example: 1) Bitflip code is $[[3,1,1]]$ code
Can map between two valid codewords with a Z operator.
$Z_1(\alpha|000\rangle + \beta|111\rangle) = \alpha|000\rangle - \beta|111\rangle$
$\alpha|0\rangle + \beta|1\rangle$ $\qquad$ $\alpha|0\rangle - \beta|1\rangle$

2) Shor code is $[[9,1,3]]$ code
Can correct all 1 qubit errors.

Exercise: Can you find 3 errors that together map between valid codewords?

The Quantum Hamming Bound

How big do we need to take n if we want to encode k qubits and protect from t-qubit errors?

By linearity we need to correct only $\{X, Y, Z\}$ on at most t-qubits to be able to correct all t-qubit errors. Assuming the code is non-degenerate (different errors map to different orthogonal subspaces), then we have

$\binom{n}{j}$ choices of qubits for j errors

3^j choices of errors

2^k dimension of encoded subspace

So $$\sum_{j=0}^{t} \binom{n}{j} 3^j 2^k \leq 2^n$$ (need to fit in all these subspaces)

quantum Hamming bound.

Remark

1) Taking $t=1$ $k=1$ we need $n \geq 5$ so Shor it not optimal

2) This bound applies only to non-degenerate codes. Degeneracy can help to be more efficient as different errors can have to same effect on codewords.

The Stabilizer Formalism I, X, Y, Z

A nice framework for building quantum codes on n-qubits.

Def^n (Pauli Group)

The Pauli group P_n on n qubits is 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.

Example $iZ \otimes X \otimes \mathbb{1} \in P_3$

$iZ_1 X_2$ shorthand notation

Properties

1) $|P_n| = 4^{n+1}$ (4^n tensor products and 4 phases)

2) $R \in P_n \Rightarrow R$ has eigenvalues $\{\pm 1, \pm i\}$ All Pauli ops have eigenvalues ± 1 and tensor products give products of eigenvalues.

3) $\forall M, N \in P_n$ either $MN = NM$ or $MN = -NM$

either commute or anticommute.

4) $M \in P_n$ then $M^2 = \pm \mathbb{1}$

Def^n (Stabilizer group)

A stabilizer group S is a subgroup of P_n such that

1) $-\mathbb{I} \notin S$
2) $[M, N] = 0 \quad \forall M, N \in S.$

Example $S = \{\mathbb{1}, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$ is a stabilizer group of P_3.

It has a minimal set of generators

$$S = \langle Z_1Z_2, Z_2Z_3 \rangle$$

any element of S can be constructed by multiplying these elements.

The first condition implies that for all $M \in S$ $M^2 = \mathbb{1}$. This ensures that the eigenvalues of M are always $\{\pm 1\}$.

Because everything commutes any $M \in S$ can be written as

$$M = S_1^{a_1} S_2^{a_2} \dots S_r^{a_r} \qquad a_i \in \{0,1\} \quad S_i \text{ - generators.}$$

so bitstring $a_1 a_2 \dots a_r$ uniquely determines M and $|S| = 2^r$.

Defn (Stabilizer Subspace)

Let S be a stabilizer group of P_n. Then $T_S \subseteq (\mathbb{C}^2)^{\otimes n}$ is called the stabilizer subspace if

$$T_S = \{ |\psi\rangle \in (\mathbb{C}^2)^{\otimes n} : M|\psi\rangle = |\psi\rangle \quad \forall M \in S \}$$

Space of vectors that are in the +1 eigenspace of each element of S.

- One can show if $|S| = 2^r$ then $\dim(T_S) = 2^{n-r}$.

Intuitively each generator cuts $\mathcal{H}$ into two spaces of equal size and thus we halve the size of the +1 eigenspace with each generator.

More formally one can show $\Pi_T = \frac{1}{2^r} \sum_{M \in S} M$ is the projector onto T.

Then $\dim(T) = \mathrm{Tr}[\Pi_T] = \frac{1}{2^r} \sum_{M \in S} \mathrm{Tr}[M] = \frac{1}{2^r} \mathrm{Tr}[\mathbb{1}] = 2^{n-r}$

Stabilizers Help to Detect Errors

The idea is that T_S will be our codespace for our QECC.

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

$$|\psi\rangle \in T_S \xrightarrow[\text{occurs}]{\text{Error}} E|\psi\rangle$$

Well now $ME|\psi\rangle = -EM|\psi\rangle = -E|\psi\rangle$ ← $E|\psi\rangle$ is an eigenvector of M with eigenvalue -1
Error moves $|\psi\rangle$ from $+1$ eigenspace to -1 eigenspace.

Note that because $|\psi\rangle$ and $E|\psi\rangle$ are contained entirely in the eigenspaces of M (orthogonal) they can be distinguished without disturbing the state.
Measuring $M \Rightarrow$ detect if E occurred.

Otherwise if we have $[E,M]=0$ then

$$ME|\psi\rangle = EM|\psi\rangle = E|\psi\rangle \quad \text{so} \quad E|\psi\rangle \in T_S \text{ and is undetectable!}$$

$$N_S = \{E \in P_n \quad : \quad [E,M]=0 \quad \forall M \in S\}$$

Set of undetectable errors is $N_S \setminus S$.

$+1$ outcome $\forall M \in S$ so think no error has occured.

Why $N_S \setminus S$?

Stabilizers can correct errors

Can we do this without disturbing the state?

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

$$\begin{array}{ccccccccc} & & M_1 & M_2 & M_3 & M_4 & M_5 & M_6 & \dots \\ \text{Syndrome} & = & (+1, & +1, & +1, & -1, & -1, & +1, & \dots \end{array}$$

we now know error anticommutes with M_4 and M_5

(Why do we need to only measure the generators?)

Lemma

Let $\mathcal{E}$ be some set of errors and suppose that for all $E_a, E_b \in \mathcal{E}$ 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 $\mathcal{E}$ is a set of correctable errors.

Proof

Suppose (1) holds then $\langle\psi_j|E_b^\dagger E_a|\psi_i\rangle = \langle\psi_j|\psi_i\rangle = 1\,\delta_{ij}$

So Knill-Laflamme conditions hold.

Suppose (2) holds then

$$\begin{aligned}\langle\psi_i|E_b^\dagger E_a|\psi_j\rangle &= \langle\psi_i|E_b^\dagger E_a M|\psi_j\rangle \\ &= -\langle\psi_i|M E_b^\dagger E_a|\psi_j\rangle \\ &= -\langle\psi_i|E_b^\dagger E_a|\psi_j\rangle\end{aligned}$$

$\Rightarrow \langle\psi_i|E_b^\dagger E_a|\psi_j\rangle = 0$

$\Rightarrow$ Knill-Laflamme conditions hold. $\boxtimes$

Th^m

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

Proof ($\Leftarrow$) Suppose $E_a^\dagger E_b \notin N(S)\setminus S$ then by previous Lemma $\mathcal{E}$ is correctable.

($\Rightarrow$) Suppose $\mathcal{E}$ is correctable but two errors produce same syndrome $\Rightarrow E_a, E_b$ commute/anticommute with same $M \in S$

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

$\Rightarrow E_a^\dagger E_b \in N(S)$ but is correctable so also belongs to S. $\boxtimes$

Bit flip as a stabilizer code

Bitflip is a $[[3,1,0]]$ code

$$S = \langle Z_1 Z_2,\ Z_2 Z_3 \rangle \qquad S \subseteq P_3$$

Codespace is $\text{span}\{|000\rangle, |111\rangle\}$ which is stabilizer subspace of S as

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

$$Z_1 Z_2 |\psi\rangle = \alpha Z_1 Z_2 |000\rangle + \beta Z_1 Z_2 |111\rangle$$

$$= \alpha|000\rangle + \beta(-1)^2|111\rangle = |\psi\rangle.$$

Same for $Z_2 Z_3$.

We want to correct $\mathcal{E} = \{X_1, X_2, X_3\}$.

One can check

X_1 produces syndrome $\begin{pmatrix} -1 \\ +1 \end{pmatrix}$

X_2 produces syndrome $\begin{pmatrix} -1 \\ -1 \end{pmatrix}$

X_3 produces syndrome $\begin{pmatrix} +1 \\ -1 \end{pmatrix}$

$\mathbb{1}$ produces syndrome $\begin{pmatrix} +1 \\ +1 \end{pmatrix}$

Completely equivalent to to parity measurements from before

$Z_1 Z_2 \to +1$ if parities of qubit 1 and 2 are same

$\to -1$ if different.

$$Z_1 Z_2 = (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes \mathbb{1}$$

$$= \Big(\underbrace{|00\rangle\langle 00| + |11\rangle\langle 11|}_{\substack{\text{even parity} \\ +1}} - \underbrace{(|01\rangle\langle 01| + |10\rangle\langle 10|)}_{\substack{\text{odd parity} \\ -1}} \Big) \otimes \mathbb{1}$$

Shor code as a Stabilizer code

$[[9,1,3]]$ code

S is generated by

$$\left.\begin{matrix} Z_1Z_2 & Z_2Z_3 \\ Z_4Z_5 & Z_5Z_6 \\ Z_7Z_8 & Z_8Z_9 \end{matrix}\right\} \text{bit flip checks}$$

$$\left.\begin{matrix} X_1X_2X_3X_4X_5X_6 \\ X_4X_5X_6X_7X_8X_9 \end{matrix}\right\} \text{phase flip checks.}$$

$|S| = 2^8$ and so $\dim(T_S) = 2$

$$T_S = \text{Span}\left\{ \tfrac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)^{\otimes 3}, \ \tfrac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)^{\otimes 3} \right\}$$

One can show that $\mathcal{E} = \{ R \in P_9 : R \text{ acts only on } 1 \text{ qubit} \}$ is a correctable set.

A more efficient code $[[5,1,3]]$

Consider a Stabilizer group on $n=5$ generated by

$$\begin{matrix} X & Z & Z & X & \mathbb{1} \\ \mathbb{1} & X & Z & Z & X \\ X & \mathbb{1} & X & Z & Z \\ Z & X & \mathbb{1} & X & Z \end{matrix}$$

$\xrightarrow{\hspace{2em}}$ cyclic shift

Any weight 2 Pauli operator anticommutes with at least one generator and so all weight 1 Pauli operators are correctable.

$16 = 3 \times 5 + 1$ possible error syndromes

4 stabilizers $=$ 4 bits of information in syndrome

$\Rightarrow$ Perfect efficiency (for non-degenerate code).

Exercise: Find a way to construct the codespace of the above code!

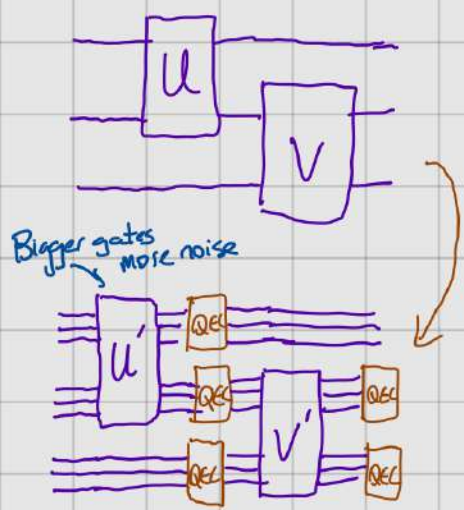
Fault tolerance & Threshold theorem (Bonus)

Quantum computing faces major problems...

* Errors are everywhere, including in the encoding / decoding and measuring steps of a QECC.
* If we want to do computations then we need to perform our gates on the encoded qubits (so the gates are more complicated).

This means error correction will introduce more errors. The idea of fault tolerance is that we need to correct more errors than we introduce!

Logical circuit



$|0\rangle_L = |000\rangle$ Encoded X is $X_1X_2X_3$ ← not always so simple form

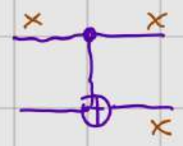
$|1\rangle_L = |111\rangle$ Encoded Z is $Z_1Z_2Z_3$

transversal gates good (just repeat on wires $U^{\otimes n}$)

Transversal gate sets depend on the encoding ← no go thm about universal sets. No transversal universal set.

* U' is now more complicated and so will produce more errors than U. However we can also now correct more errors!
* QEC modules can also introduce errors, we have to hope not too many so they can be corrected by the next QEC module.

* Some gates will propagate errors, ex.



need them to not spread too fast...

<u>Threshold theorem (Aharonov Ben'or)</u> [Informal]

Assuming some 'reasonable' noise model (Eg. iid errors) then $\exists$ a universal constant κ such that if error rate is $p \leq \kappa$ then for any logical circuit C with T gates we can build a noisy physical circuit C' with T' gates such that C and C' give the same results and $T' = T\,O(\mathrm{polylog}(T))$

κ depends on error model $\qquad$ $\kappa \sim 10^{-3}$ for some models.

Stabilizer codes from Linear ECCs.

Bonus

<u>Def^n</u> A classical linear code C is a set of bitstrings such that if $x, y \in C \Rightarrow x+y \in C$

Can be defined via generator matrix $G \in M_{k \times n}(\mathbb{F}_2)$
Given logical vector v (bitstring of length k) we get a codeword (bitstring of length n) $G^T v$.

Rep code
$G = (1\ 1\ 1)$

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

<u>Ex (Hamming Code)</u>

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

$k=4$
$n=7$

$[7,4,3]$ code

Hamming distance : # places where bitstrings differ.
<u>Distance of linear code</u> minimum Hamming distance between any pair of codewords (equivs smallest weight of a codeword)

(n,k,d) code.

For a linear code a <u>parity check</u> matrix H is a matrix of maximal rank st. $HG^T = 0$.

$\Rightarrow HG^T v = \underline{0}$ (if an error occurs to $G^T v$ then $H\mathcal{E}(G^T v) \neq 0$ ← checks for error

codeword $x \xrightarrow{\text{error}} x+e$

then $H(x+e) = Hx + He = He$ ← error syndrome.

codewords are $\ker(H)$
$\{x : Hx = 0\}$

Ex (Hamming code):

$$H = \begin{pmatrix} \overbrace{1 & 1 & 1 & 1}^{\text{1st 4 bits have even parity.}} & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

e_i

Single bit errors have syndromes which are the ith column.
$\Rightarrow$ All single bit errors can be corrected !

Connection to Stabilizers

$$H \longrightarrow \begin{matrix} Z & Z & Z & Z & I & I & I \\ Z & Z & I & I & Z & Z & I \\ Z & I & Z & I & Z & I & Z \end{matrix}$$

Should be able to correct single bit flip errors

Could do same with X to get phase flip correcting code.

How to combine?

CSS construction

Take two classical linear codes. C_1 & C_2 with P-check matrice H_1 and H_2.

$$H_1 \to 1 \to Z$$
$$H_2 \to 1 \to X$$

take stabilizer generated by these things.

Ex: $C_1 = C_2 =$ Hamming $[7,4,3]$

then we get

identifies and XZ error

identifies any X error
$$\begin{matrix} Z & Z & Z & Z & 1 & 1 & 1 \\ Z & Z & 1 & 1 & Z & Z & 1 \\ Z & 1 & Z & 1 & Z & 1 & Z \end{matrix}$$

identifies any Z error
$$\begin{matrix} X & X & X & X & 1 & 1 & 1 \\ X & X & 1 & 1 & X & X & 1 \\ X & 1 & X & 1 & X & 1 & X \end{matrix}$$

generates Abelian group
6 generators so
1 logical qubit

$[[7,1,3]]$ code

corrects all 1 qubit errors.

This construction works for any classical codes C_1, C_2. as long as above group is Abelian. can show that this is iff

$v \cdot w = 0 \leftrightarrow$ # places where same is even

v is row in H_1
w is row in H_2.