9. Combating noise: quantum error correcting codes

(NC 10.1-10.3, 10.5, M 5, KLM 10)

(a) Classical noise model

(b) 3-bit repetition code

(c) Quantum noise model

(d) Quantum 3-bit repetition code for X errors

(e) Shor 9-bit code for arbitrary Pauli error

(g) Discretization and sufficient conditions for QECC

(h) Stabilizer formalism -- quantum parity checks !

5-bit code

(i) Shor 9-bit code reloaded

(j) Sufficient conditions for QECC for stabilizer codes

(l) 7-bit Steane code

(m) Erasure errors, q secret sharing, AdS/CFT corr

5-qubit code for arbitrary 1-qubit error

Consider 4 commuting Pauli's (generators) in 5 qubits:

G1 = XZZXI
G2 = IXZZX
G3 = XIXZZ
G4 = ZXIXZ

5-qubit code for arbitrary 1-qubit error

Consider 4 commuting Pauli's (generators) in 5 qubits:

G1 = XZZXI
G2 = IXZZX
G3 = XIXZZ
G4 = ZXIXZ

They generate a 16 element stabilizer group S, and a 2-dim QECC C (so 1 qubit is encoded in 5).

Is there cyclic symmetry in the code?

(a) yes, (b) no.

5-qubit code for arbitrary 1-qubit error

Consider 4 commuting Pauli's (generators) in 5 qubits:

G1 = XZZXI
G2 = IXZZX
G3 = XIXZZ
G4 = ZXIXZ

They generate a 16 element stabilizer group S,
and a 2-dim QECC C (so 1 qubit is encoded in 5).

Is there cyclic symmetry in the code?

(a) yes, (b) no.

Yes, because G1 G2 G3 G4 = ZZXIX.

5-qubit code for arbitrary 1-qubit error

G1 = XZZXI
G2 = IXZZX
G3 = XIXZZ
G4 = ZXIXZ

Will verify ability to correct
1-qubit Pauli errors in 2 ways:

1 Pauli error

(5 positions, 3 types) no error

$5 \times 3 + 1$

5-qubit code for arbitrary 1-qubit error

G1 = XZZXI
G2 = IXZZX
G3 = XIXZZ
G4 = ZXIXZ

Will verify ability to correct
1-qubit Pauli errors in 2 ways:

1 Pauli error
(5 positions, 3 types)

no error

$5 \times 3 + 1$

A5 Q1

Method 1: list the syndromes (eigenvalues of G1-G4) for the 16 possible Pauli errors we need to correct, and check that they are distinct.

5-qubit code for arbitrary 1-qubit error

G1 = XZZXI
G2 = IXZZX
G3 = XIXZZ
G4 = ZXIXZ

Will verify ability to correct 1-qubit Pauli errors in 2 ways:

1 Pauli error (5 positions, 3 types) no error

5 × 3 + 1

A5 Q1

Method 1: list the syndromes (eigenvalues of G1-G4) for the 16 possible Pauli errors we need to correct, and check that they are distinct.

16 cases to check

	I	X1	X2	Y5
G1 = XZZXI	+	+	-	+
G2 = IXZZX	+	+	+	-
G3 = XIXZZ	+	+	+	-
G4 = ZXIXZ	+	-	+	-

Remark: the 16 errors take the 2-dim codespace to orthogonal spaces occupying $16*2 = 32$ dims, so, the ambient space is completely used.

Remark: the 16 errors take the 2-dim codespace to orthogonal spaces occupying 16*2 = 32 dims, so, the ambient space is completely used.

5-qubit is the shortest blocklength to encode 1 qubit & corrects an arbitrary 1-qubit error.

Proof: tricky since it may not be necessary to distinguish the errors (e.g., Z's in 9-bit Shor code). (Out of scope, see Gottesman thesis if interested.)

Remark: the 16 errors take the 2-dim codespace to orthogonal spaces occupying 16*2 = 32 dims, so, the ambient space is completely used.

5-qubit is the shortest blocklength to encode 1 qubit & corrects an arbitrary 1-qubit error.

Proof: tricky since it may not be necessary to distinguish the errors (e.g., Z's in 9-bit Shor code). (Out of scope, see Gottesman thesis if interested.)

Checking correctness of 5-bit code is different from "understanding why it works". The second proof of correctness relies on special sufficient QECC condition for stabilizer codes.

9. Combating noise: quantum error correcting codes

(NC 10.1-10.3, 10.5, M 5, KLM 10)

(a) Classical noise model

(b) 3-bit repetition code

(c) Quantum noise model

(d) Quantum 3-bit repetition code for X errors

(e) Shor 9-bit code for arbitrary Pauli error

(g) Discretization and sufficient conditions for QECC

(h) Stabilizer formalism -- quantum parity checks !

(i) Shor 9-bit code reloaded

5-bit code

(j) Sufficient conditions for QECC for stabilizer codes

(l) 7-bit Steane code

(m) Erasure errors, q secret sharing, AdS/CFT corr

QECC condition for stabilizer codes and Pauli errors

Let G1, G2, ..., Gm be the generators for the stabilizer group for a stabilizer code C.

Let E1, E2, ..., Er be a set of Pauli matrices.

Then, any quantum operation with Kraus operators in the span of E1, E2, ..., Er is correctible on C if

$\forall\, i \neq j$, $\exists\, l$ s.t. $E_i E_j$ anticommutes with G_l.

QECC condition for stabilizer codes and Pauli errors

Let G1, G2, ..., Gm be the generators for the stabilizer group for a stabilizer code C.

Let E1, E2, ..., Er be a set of Pauli matrices.

Then, any quantum operation with Kraus operators in the span of E1, E2, ..., Er is correctible on C if

$\forall\, i \neq j$, $\exists\, \ell$ s.t. $E_i E_j$ anticommutes with G_ℓ.

Proof: let P be the projector onto the codespace C.

Note $P = \left(\frac{I+G_1}{2}\right)\left(\frac{I+G_2}{2}\right)\left(\frac{I+G_3}{2}\right) \cdots \left(\frac{I+G_m}{2}\right)$

QECC condition for stabilizer codes and Pauli errors

Let G1, G2, ..., Gm be the generators for the stabilizer group for a stabilizer code C.

Let E1, E2, ..., Er be a set of Pauli matrices.

Then, any quantum operation with Kraus operators in the span of E1, E2, ..., Er is correctible on C if

$\forall i \neq j$, $\exists l$ s.t. $E_i E_j$ anticommutes with G_l.

Proof: let P be the projector onto the codespace C.

Note $P = \left(\frac{I+G_1}{2}\right)\left(\frac{I+G_2}{2}\right)\left(\frac{I+G_3}{2}\right) \cdots \left(\frac{I+G_m}{2}\right)$

So, $\forall i = 1, 2, \ldots, m$ $[P, G_i] = 0$.

commutator
$[A,B]=AB-BA$

anticommutator
$\{A,B\}=AB+BA$

For $i \neq j$, $\exists\, \ell$ s.t. $\{G_\ell, E_i E_j\} = 0$

For $i \neq j$, $\exists \ell$ s.t. $\{G_\ell, E_i E_j\} = 0$

$\forall |\psi\rangle$, $P E_i E_j P |\psi\rangle$ ($|\psi\rangle \in A$ the ambient space)

For $i \neq j$, $\exists \ell$ s.t. $\{G_\ell, E_i E_j\} = 0$

$\forall |\psi\rangle$, $P E_i E_j P |\psi\rangle$ ($|\psi\rangle \in A$ the ambient space)

$= P E_i E_j G_\ell P |\psi\rangle$ ($\because P|\psi\rangle \in C$)

For $i \neq j$, $\exists \ell$ s.t. $\{G_\ell, E_i E_j\} = 0$

$$\forall |\psi\rangle, \; P E_i E_j P |\psi\rangle \qquad (|\psi\rangle \in A \text{ the ambient space})$$

$$= P E_i E_j G_\ell P |\psi\rangle \qquad (\because P|\psi\rangle \in C)$$

$$= - P G_\ell E_i E_j P |\psi\rangle \qquad (\because \{G_\ell, E_i E_j\} = 0)$$

For $i \neq j$, $\exists\, \ell$ s.t. $\{G_\ell, E_i E_j\} = 0$

$$\forall |\psi\rangle,\ P E_i E_j P |\psi\rangle \qquad (|\psi\rangle \in A \text{ the ambient space})$$

$$= P E_i E_j G_\ell P |\psi\rangle \qquad (\because P|\psi\rangle \in C)$$

$$= -P G_\ell E_i E_j P |\psi\rangle \qquad (\because \{G_\ell, E_i E_j\} = 0)$$

$$= -G_\ell P E_i E_j P |\psi\rangle \qquad (\because [P, G_\ell] = 0)$$

For $i \neq j$, $\exists \ell$ s.t. $\{G_\ell, E_i E_j\} = 0$

$\forall |\psi\rangle$, $P E_i E_j P |\psi\rangle$ ($|\psi\rangle \in A$ the ambient space)

$= P E_i E_j G_\ell P |\psi\rangle$ ($\because P|\psi\rangle \in C$)

$= - P G_\ell E_i E_j P |\psi\rangle$ ($\because \{G_\ell, E_i E_j\} = 0$)

$= - G_\ell P E_i E_j P |\psi\rangle$ ($\because [P, G_\ell] = 0$)

$= - P E_i E_j P |\psi\rangle$ ($\because P E_i E_j P |\psi\rangle \in C$)

For $i \neq j$, $\exists\, \ell$ s.t. $\{G_\ell, E_i E_j\} = 0$

$$
\begin{aligned}
\forall |\psi\rangle,\ & P E_i E_j P |\psi\rangle & & (|\psi\rangle \in A \text{ the ambient space}) \\
&= P E_i E_j G_\ell P |\psi\rangle & & (\because P|\psi\rangle \in C) \\
&= - P G_\ell E_i E_j P |\psi\rangle & & (\because \{G_\ell, E_i E_j\} = 0) \\
&= - G_\ell P E_i E_j P |\psi\rangle & & (\because [P, G_\ell] = 0) \\
&= - P E_i E_j P |\psi\rangle & & (\because P E_i E_j P |\psi\rangle \in C)
\end{aligned}
$$

$\therefore\ P E_i E_j P |\psi\rangle = 0$

For $i \neq j$, $\exists \, l$ s.t. $\{G_l, E_i E_j\} = 0$

$\forall |\psi\rangle$, $P E_i E_j P |\psi\rangle$ $\quad$ ($|\psi\rangle \in A$ the ambient space)

$= P E_i E_j G_l P |\psi\rangle$ $\quad$ ($\because P|\psi\rangle \in C$)

$= - P G_l E_i E_j P |\psi\rangle$ $\quad$ ($\because \{G_l, E_i E_j\} = 0$)

$= - G_l P E_i E_j P |\psi\rangle$ $\quad$ ($\because [P, G_l] = 0$)

$= - P E_i E_j P |\psi\rangle$ $\quad$ ($\because P E_i E_j P |\psi\rangle \in C$)

$\therefore$ $P E_i E_j P |\psi\rangle = 0$

$\therefore$ $P E_i E_j P = 0$

For $i \neq j$, $\exists \ell$ s.t. $\{G_\ell, E_i E_j\} = 0$

$\forall |\psi\rangle$, $P E_i E_j P |\psi\rangle$ ($|\psi\rangle \in A$ the ambient space)

$= P E_i E_j G_\ell P |\psi\rangle$ ($\because P|\psi\rangle \in C$)

$= - P G_\ell E_i E_j P |\psi\rangle$ ($\because \{G_\ell, E_i E_j\} = 0$)

$= - G_\ell P E_i E_j P |\psi\rangle$ ($\because [P, G_\ell] = 0$)

$= - P E_i E_j P |\psi\rangle$ ($\because P E_i E_j P |\psi\rangle \in C$)

$\therefore P E_i E_j P |\psi\rangle = 0$

$\therefore P E_i E_j P = 0$

For $i = j$, $P E_i E_j P = P$

So, the sufficient condition for QECC is satisfied.

QECC condition for stabilizer codes and Pauli errors

Let G1, G2, ..., Gm be the generators for the stabilizer group for a stabilizer code C.

Let E1, E2, ..., Er be a set of Pauli matrices.

Then, any quantum operation with Kraus operators in the span of E1, E2, ..., Er is correctible on C if

$\forall i \neq j$, $\exists l$ s.t. $E_i E_j$ anticommutes with G_l.

Next: showing the above abstract condition implies that the errors have distinct +/- signs when we measure G1, G2, ..., Gm, leading to a simple algorithm to identify the error.

Claim: measuring G1,G2,...,Gm effects a refinement of the measurement with projectors $E_i P E_i$.

Claim: measuring G1,G2,...,Gm effects a refinement of the measurement with projectors $E_i P E_i$.

Proof: the measurement of G1, G2, ..., Gm is described by 2^m projectors $\left(\frac{I \pm G_1}{2}\right)\left(\frac{I \pm G_2}{2}\right)\left(\frac{I \pm G_3}{2}\right) \cdots \left(\frac{I \pm G_m}{2}\right)$.

Claim: measuring G1,G2,...,Gm effects a refinement of the measurement with projectors $E_i P E_i$.

Proof: the measurement of G1, G2, ..., Gm is described by 2^m projectors $\left(\frac{I \pm G_1}{2}\right)\left(\frac{I \pm G_2}{2}\right)\left(\frac{I \pm G_3}{2}\right) \cdots \left(\frac{I \pm G_m}{2}\right)$.

$\forall i$ let $c_{il} = \begin{cases} +1 & \text{if } [E_i, G_l] = 0 \\ -1 & \text{if } \{E_i, G_l\} = 0 \end{cases}$

Claim: measuring G1,G2,...,Gm effects a refinement of the measurement with projectors $E_i P E_i$.

Proof: the measurement of G1, G2, ..., Gm is described by 2^m projectors $\left(\frac{I \pm G_1}{2}\right)\left(\frac{I \pm G_2}{2}\right)\left(\frac{I \pm G_3}{2}\right) \cdots \left(\frac{I \pm G_m}{2}\right)$.

$\forall i$ let $c_{il} = \begin{cases} +1 & \text{if } [E_i, G_l] = 0 \\ -1 & \text{if } \{E_i, G_l\} = 0 \end{cases}$

$$E_i P E_i = E_i \left(\frac{I+G_1}{2}\right)\left(\frac{I+G_2}{2}\right)\left(\frac{I+G_3}{2}\right) \cdots \left(\frac{I+G_m}{2}\right) E_i$$

direct substitution

Claim: measuring G1,G2,...,Gm effects a refinement of the measurement with projectors $E_i P E_i$.

Proof: the measurement of G1, G2, ..., Gm is described by 2^m projectors $\left(\frac{I \pm G_1}{2}\right)\left(\frac{I \pm G_2}{2}\right)\left(\frac{I \pm G_3}{2}\right)\cdots\left(\frac{I \pm G_m}{2}\right)$.

$\forall i$ let $c_{il} = \begin{cases} +1 & \text{if } [E_i, G_l] = 0 \\ -1 & \text{if } \{E_i, G_l\} = 0 \end{cases}$

$$E_i P E_i = E_i \left(\frac{I+G_1}{2}\right)\left(\frac{I+G_2}{2}\right)\left(\frac{I+G_3}{2}\right)\cdots\left(\frac{I+G_m}{2}\right) E_i$$

$$= E_i \left(\frac{I+G_1}{2}\right) E_i E_i \left(\frac{I+G_2}{2}\right) E_i E_i \left(\frac{I+G_3}{2}\right)\cdots\left(\frac{I+G_m}{2}\right) E_i$$

insert identity

Claim: measuring G1,G2,...,Gm effects a refinement of the measurement with projectors $E_i P E_i$.

Proof: the measurement of G1, G2, ..., Gm is described by 2^m projectors $\left(\frac{I \pm G_1}{2}\right)\left(\frac{I \pm G_2}{2}\right)\left(\frac{I \pm G_3}{2}\right) \cdots \left(\frac{I \pm G_m}{2}\right)$.

$\forall i$ let $c_{il} = \begin{cases} +1 & \text{if } [E_i, G_l] = 0 \\ -1 & \text{if } \{E_i, G_l\} = 0 \end{cases}$

$$E_i P E_i = E_i \left(\frac{I+G_1}{2}\right)\left(\frac{I+G_2}{2}\right)\left(\frac{I+G_3}{2}\right) \cdots \left(\frac{I+G_m}{2}\right) E_i$$

$$= E_i \left(\frac{I+G_1}{2}\right) E_i E_i \left(\frac{I+G_2}{2}\right) E_i E_i \left(\frac{I+G_3}{2}\right) \cdots \left(\frac{I+G_m}{2}\right) E_i$$

$$= \left(\frac{I+c_{i1}G_1}{2}\right)\left(\frac{I+c_{i2}G_2}{2}\right)\left(\frac{I+c_{i3}G_3}{2}\right) \cdots \left(\frac{I+c_{im}G_m}{2}\right)$$

Claim: measuring G1,G2,...,Gm effects a refinement of the measurement with projectors $E_i P E_i$.

Proof: the measurement of G1, G2, ..., Gm is described by 2^m projectors $\left(\frac{I\pm G_1}{2}\right)\left(\frac{I\pm G_2}{2}\right)\left(\frac{I\pm G_3}{2}\right)\cdots\left(\frac{I\pm G_m}{2}\right)$.

$\forall i$ let $c_{il} = \begin{cases} +1 & \text{if } [E_i, G_l] = 0 \\ -1 & \text{if } \{E_i, G_l\} = 0 \end{cases}$

$$E_i P E_i = E_i \left(\frac{I+G_1}{2}\right)\left(\frac{I+G_2}{2}\right)\left(\frac{I+G_3}{2}\right)\cdots\left(\frac{I+G_m}{2}\right) E_i$$

$$= E_i \left(\frac{I+G_1}{2}\right) E_i E_i \left(\frac{I+G_2}{2}\right) E_i E_i \left(\frac{I+G_3}{2}\right)\cdots\left(\frac{I+G_m}{2}\right) E_i$$

$$= \left(\frac{I+c_{i1}G_1}{2}\right)\left(\frac{I+c_{i2}G_2}{2}\right)\left(\frac{I+c_{i3}G_3}{2}\right)\cdots\left(\frac{I+c_{im}G_m}{2}\right)$$

which is one of the projectors when measuring G1,G2,...,Gm.

Claim: measuring G1,G2,...,Gm effects a refinement of the measurement with projectors $E_i P E_i$.

Proof: the measurement of G1, G2, ..., Gm is described by 2^m projectors $\left(\frac{I \pm G_1}{2}\right)\left(\frac{I \pm G_2}{2}\right)\left(\frac{I \pm G_3}{2}\right) \cdots \left(\frac{I \pm G_m}{2}\right)$.

$\forall i$ let $c_{il} = \begin{cases} +1 & \text{if } [E_i, G_l] = 0 \\ -1 & \text{if } \{E_i, G_l\} = 0 \end{cases}$

$$E_i P E_i = E_i \left(\frac{I+G_1}{2}\right)\left(\frac{I+G_2}{2}\right)\left(\frac{I+G_3}{2}\right) \cdots \left(\frac{I+G_m}{2}\right) E_i$$

$$= E_i \left(\frac{I+G_1}{2}\right) E_i E_i \left(\frac{I+G_2}{2}\right) E_i E_i \left(\frac{I+G_3}{2}\right) \cdots \left(\frac{I+G_m}{2}\right) E_i$$

$$= \left(\frac{I+c_{i1}G_1}{2}\right)\left(\frac{I+c_{i2}G_2}{2}\right)\left(\frac{I+c_{i3}G_3}{2}\right) \cdots \left(\frac{I+c_{im}G_m}{2}\right)$$

which is one of the projectors when measuring G1,G2,...,Gm.

Note $E_i P E_i$ projects onto c_{i1} eigenspace of G_1, and c_{i2} eigenspace of G_2, ..., c_{im} eigenspace of G_m.

The list $c_{i1}, c_{i2}, \ldots, c_{im}$ is the syndrome (list of outcomes when measuring G1, ...,Gm) if Ei happens.

$\boxed{\text{The list } c_{i1}, c_{i2}, \ldots, c_{im} \text{ is the syndrome (list of outcomes when measuring G1, ...,Gm) if Ei happens.}}$

Furthermore, for $i \neq j$,

if $E_i E_j$ anticommute with some G_ℓ

then, exactly one of Ei, Ej commute with G ℓ,

and one of Ei, Ej anticommute with G ℓ.

$\boxed{\text{The list } c_{i1}, c_{i2}, \ldots, c_{im} \text{ is the syndrome (list of outcomes when measuring G1, ..., Gm) if Ei happens.}}$

Furthermore, for $i \neq j$,

if $E_i E_j$ anticommute with some G_ℓ

then, exactly one of Ei, Ej commute with G$_\ell$,

and one of Ei, Ej anticommute with G $_\ell$.

So, $c_{i\ell} \neq c_{j\ell}$ and Ei, Ej must have different ℓ-th in their syndromes.

The list $c_{i1}, c_{i2}, \cdots, c_{im}$ is the syndrome (list of outcomes when measuring G1, ...,Gm) if Ei happens.

Furthermore, for $i \neq j$,

if $E_i E_j$ anticommute with some G_ℓ

then, exactly one of Ei, Ej commute with G$_\ell$,

and one of Ei, Ej anticommute with G $_\ell$.

So, $c_{i\ell} \neq c_{j\ell}$ and Ei, Ej must have different ℓ-th in their syndromes.

This is an algorithmic way to see and use the sufficient QECC condition $\forall i \neq j, \exists \ell$ s.t $\{E_i E_j, G_\ell\} = 0$

9. Combating noise: quantum error correcting codes

(NC 10.1-10.3, 10.5, M 5, KLM 10)

(a) Classical noise model

(b) 3-bit repetition code

(c) Quantum noise model

(d) Quantum 3-bit repetition code for X errors

(e) Shor 9-bit code for arbitrary Pauli error

(g) Discretization and sufficient conditions for QECC

(h) Stabilizer formalism -- quantum parity checks !

5-bit code

(i) Shor 9-bit code reloaded

(j) Sufficient conditions for QECC for stabilizer codes

(l) 7-bit Steane code

(m) Erasure errors, q secret sharing, AdS/CFT corr

Method 2 to verify that the 5-bit code corrects up to 1 Pauli error, using QECC condition for stabilizer codes

Method 2 to verify that the 5-bit code corrects up to 1 Pauli error, using QECC condition for stabilizer codes

Consider all possible $E_i E_j$,
for any pair of 0- or 1-qubit Pauli errors E_i, E_j with $i \neq j$.

Method 2 to verify that the 5-bit code corrects up to 1 Pauli error, using QECC condition for stabilizer codes

Consider all possible $E_i E_j$,
for any pair of 0- or 1-qubit Pauli errors E_i, E_j with $i \neq j$.

$\because$ $i \neq j$ at least one of $E_i, E_j \neq I$. WLOG, $E_i \neq I$.

Method 2 to verify that the 5-bit code corrects up to 1 Pauli error, using QECC condition for stabilizer codes

Consider all possible $E_i E_j$,

for any pair of 0- or 1-qubit Pauli errors E_i, E_j with $i \neq j$.

$\because$ $i \neq j$ at least one of $E_i, E_j \neq I$. WLOG, $E_i \neq I$.

$\therefore$ E_i is a 1-qubit Pauli error. By cyclic symmetry,

E_i acts nontrivially on the 1st qubit.

Method 2 to verify that the 5-bit code corrects up to 1 Pauli error, using QECC condition for stabilizer codes

Consider all possible $E_i E_j$,

for any pair of 0- or 1-qubit Pauli errors E_i, E_j with $i \neq j$.

$\because$ $i \neq j$ at least one of $E_i, E_j \neq I$. WLOG, $E_i \neq I$.

$\therefore$ E_i is a 1-qubit Pauli error. By cyclic symmetry,

E_i acts nontrivially on the 1st qubit.

Case 1: Ej = I, or Ej is an error on the 1st qubit,

Method 2 to verify that the 5-bit code corrects up to 1 Pauli error, using QECC condition for stabilizer codes

Consider all possible $E_i E_j$,
for any pair of 0- or 1-qubit Pauli errors E_i, E_j with $i \neq j$.

$\because$ $i \neq j$ at least one of $E_i, E_j \neq I$. WLOG, $E_i \neq I$.
$\therefore$ E_i is a 1-qubit Pauli error. By cyclic symmetry,
E_i acts nontrivially on the 1st qubit.

Case 1: Ej = I, or Ej is an error on the 1st qubit,
$E_i E_j$ acts nontrivially only on the 1st qubit.

Method 2 to verify that the 5-bit code corrects up to 1 Pauli error, using QECC condition for stabilizer codes

Consider all possible $E_i E_j$,
for any pair of 0- or 1-qubit Pauli errors E_i, E_j with $i \neq j$.

$\because$ $i \neq j$ at least one of $E_i, E_j \neq I$. WLOG, $E_i \neq I$.
$\therefore$ E_i is a 1-qubit Pauli error. By cyclic symmetry,
E_i acts nontrivially on the 1st qubit.

Case 1: Ej = I, or Ej is an error on the 1st qubit,
$E_i E_j$ acts nontrivially only on the 1st qubit.

G1 = XZZXI
G2 = IXZZX
G3 = XIXZZ
G4 = ZXIXZ

$\therefore$ $E_i E_j$ = X, Y, or Z on 1st qubit, which anticommutes with G4, G1, G1 resp.

Case 2: Ej acts nontrivially on one of qubits 2-5

Case 1: Ej = I, or Ej is an error on the 1st qubit, Case 2: Ej acts nontrivially on one of qubits 2-5, thus anticommutes with one of

G2 = IXZZX

G1 G3 = IZYYZ

since in each of columns 2-5, we have 2 DIFFERENT Paulis, and Ej cannot commute with both.

e.g., if Ej acts nontrivially on the 2nd qubit,

then Ej = IXIII or IYIII anticommutes with G1G3

Ej = IZIII anticommutes with G2.

Case 2: Ej acts nontrivially on one of qubits 2-5, thus anticommutes with one of

G2 = IXZZX

G1 G3 = IZYYZ

since in each of columns 2-5, we have 2 DIFFERENT Paulis, and Ej cannot commute with both.

e.g., if Ej acts nontrivially on the 2nd qubit,

then Ej = IXIII or IYIII anticommutes with G1G3

Ej = IZIII anticommutes with G2.

Also Ei acts only on qubit 1 and thus commutes with G2 and G1G3. Together Ei Ej must anticommute with at least one of G2 and G1G3 (then one of G1 or G3).

□

What are the codewords for the code stabilizer by

G1 = XZZXI
G2 = IXZZX
G3 = XIXZZ
G4 = ZXIXZ ?

The generators only specify a 2-dim codespace C.
Any basis of C can be $\{|0_L\rangle, |1_L\rangle\}$.

One way to specify $\{|0_L\rangle, |1_L\rangle\}$ is to specify Z_L, X_L.

Logical operations for a stabilizer code

Theorem: Let G1, G2, ..., Gm be the generator of a stabilizer group, U a unitary, all acting on n qubits, C the stabilizer code, and P the projector onto C.

If U commutes with all the generators, then, U is a logical operation on the codespace.

Logical operations for a stabilizer code

Theorem: Let G1, G2, ..., Gm be the generator of a stabilizer group, U a unitary, all acting on n qubits, C the stabilizer code, and P the projector onto C.

If U commutes with all the generators, then, U is a logical operation on the codespace.

What characterizes a logical operator?
Takes any codeword to a codeword.

Logical operations for a stabilizer code

Theorem: Let G1, G2, ..., Gm be the generator of a stabilizer group, U a unitary, all acting on n qubits, C the stabilizer code, and P the projector onto C.

If U commutes with all the generators, then, U is a logical operation on the codespace.

$\boxed{\begin{array}{l}\text{What characterizes a logical operator?}\\ \text{Takes any codeword to a codeword.}\\ \forall\, |\psi_L\rangle \in C, \quad U|\psi_L\rangle \in C\end{array}}$

Logical operations for a stabilizer code

Theorem: Let G1, G2, ..., Gm be the generator of a stabilizer group, U a unitary, all acting on n qubits, C the stabilizer code, and P the projector onto C.

If U commutes with all the generators, then, U is a logical operation on the codespace.

What characterizes a logical operator?
Takes any codeword to a codeword.

$$\forall |\psi_L\rangle \in C, \quad \underbrace{U|\psi_L\rangle \in C}$$

this holds iff $P\,U|\psi_L\rangle = U|\psi_L\rangle$

Logical operations for a stabilizer code

Theorem: Let G1, G2, ..., Gm be the generator of a stabilizer group, U a unitary, all acting on n qubits, C the stabilizer code, and P the projector onto C.

If U commutes with all the generators, then, U is a logical operation on the codespace.

What characterizes a logical operator?
Takes any codeword to a codeword.

$\forall |\psi_L\rangle \in C, \quad \underbrace{U|\psi_L\rangle \in C}$

this holds iff $P\,U|\psi_L\rangle = U|\psi_L\rangle$

Proof (Theorem): $P = \frac{1}{2}(I+G_1)\frac{1}{2}(I+G_2)\cdots\frac{1}{2}(I+G_m)$

By hypothesis, PU=UP.

Logical operations for a stabilizer code

Theorem: Let G1, G2, ..., Gm be the generator of a stabilizer group, U a unitary, all acting on n qubits, C the stabilizer code, and P the projector onto C.

If U commutes with all the generators, then, U is a logical operation on the codespace.

What characterizes a logical operator?
Takes any codeword to a codeword.

$$\forall |\psi_L\rangle \in C, \quad \underbrace{U|\psi_L\rangle \in C}_{\text{this holds iff } P\,U|\psi_L\rangle = U|\psi_L\rangle}$$

Proof (Theorem): $P = \frac{1}{2}(I+G_1)\frac{1}{2}(I+G_2)\cdots\frac{1}{2}(I+G_m)$, PU=UP.

So, $\forall |\psi_L\rangle \in C, \quad P\,U|\psi_L\rangle \underset{PU=UP}{=} U\,P|\psi_L\rangle \underset{|\psi_L\rangle \in C}{=} U|\psi_L\rangle \quad \therefore U|\psi_L\rangle \in C$

The theorem can be strengthened:
If UP = PU, then U is a logical operation on C.

The theorem can be strengthened:
If UP = PU, then U is a logical operation on C.

Since $P = \frac{1}{2}(I+G_1)\frac{1}{2}(I+G_2)\cdots\frac{1}{2}(I+G_m) = \frac{1}{2^m}\sum_{M\in S} M$,

$\{UMU^\dagger : M \in S\} = S \Rightarrow$ UP = PU.

The theorem can be strengthened:
If UP = PU, then U is a logical operation on C.

Since $P = \frac{1}{2}(I+G_1)\frac{1}{2}(I+G_2)\cdots\frac{1}{2}(I+G_m) = \frac{1}{2^m}\sum_{M\in S} M$,

$\{UMU^\dagger : M \in S\} = S \Rightarrow$ UP = PU.

So U is a logical operation if conjugating the elements of S by U permutes them (special case: U commutes with each generator $UMU^\dagger = M$).

Logical operations for the 5-qubit code:

G1 = XZZXI
G2 = IXZZX
G3 = XIXZZ
G4 = ZXIXZ

By inspection, both XXXXX, ZZZZZ commute with all the generators, are hermitian, and square to IIIII.

holds for any n-qubit Pauli's, one more reason why we choose them

Logical operations for the 5-qubit code:

G1 = XZZXI
G2 = IXZZX
G3 = XIXZZ
G4 = ZXIXZ

By inspection, both XXXXX, ZZZZZ commute with all the generators, are hermitian, and square to IIIII.

holds for any n-qubit Pauli's, one more reason why we choose them

Furthermore, they anticommute with one another. So, they can be chosen as X_L, Z_L.

doesn't matter which one is which, the choice amounts to exchanging

$\{|0_L\rangle, |1_L\rangle\}$ and $\{|+_L\rangle, |-_L\rangle\}$

Logical operations for the 5-qubit code:

G1 = XZZXI
G2 = IXZZX
G3 = XIXZZ
G4 = ZXIXZ

By inspection, both XXXXX, ZZZZZ commute with all the generators, are hermitian, and square to IIIII.

holds for any n-qubit Pauli's, one more reason why we choose them

Furthermore, they anticommute with one another.
So, they can be chosen as X_L, Z_L.

doesn't matter which one is which, the choice amounts to exchanging $\{|0_L\rangle, |1_L\rangle\}$ and $\{|+_L\rangle, |-_L\rangle\}$

If we only specify Z , there is a free relative phase between $|0_L\rangle, |1_L\rangle$, so we pick X_L, Z_L together.

Codewords for stabilizer code of 2-dim on n qubits

$$|0_L\rangle\langle 0_L| = \underbrace{\frac{1}{2}(I+G_1)\frac{1}{2}(I+G_2)\cdots\frac{1}{2}(I+G_{n-1})}_{=P}\ \underbrace{\frac{1}{2}(I+Z_L)}_{=|0_L\rangle\langle 0_L|}$$

Codewords for stabilizer code of 2-dim on n qubits

$$|0_L\rangle\langle 0_L| = \frac{1}{2}(I+G_1)\frac{1}{2}(I+G_2)\cdots\frac{1}{2}(I+G_{n-1})\frac{1}{2}(I+Z_L)$$

Easiest to take any state $|\psi\rangle$, and find $|\psi'\rangle = |0_L\rangle\langle 0_L|\psi\rangle$.

Then, $|0_L\rangle = \dfrac{|\psi'\rangle}{\||\psi'\rangle\|}$, (up to an overphase).

Codewords for stabilizer code of 2-dim on n qubits

$$|0_L\rangle\langle 0_L| = \frac{1}{2}(I+G_1)\frac{1}{2}(I+G_2)\cdots\frac{1}{2}(I+G_{n-1})\frac{1}{2}(I+Z_L)$$

Easiest to take any state $|\psi\rangle$, and find $|\psi'\rangle = |0_L\rangle\langle 0_L|\psi\rangle$.

Then, $|0_L\rangle = \dfrac{|\psi'\rangle}{\| |\psi'\rangle \|}$, (up to an overphase).

Do not find $|1_L\rangle$ by the above method.

Instead, take $|1_L\rangle = X_L|0_L\rangle$ to ensure the relative phase between $|0_L\rangle, |1_L\rangle$ is correct.

Codewords for the 5-qubit code:

$$|0_L\rangle\langle 0_L| = \frac{1}{2}(I+G_1)\,\frac{1}{2}(I+G_2)\,\frac{1}{2}(I+G_3)\,\frac{1}{2}(I+G_4)\,\frac{1}{2}(I+Z_L)$$

Take $|\psi\rangle = |00000\rangle$.

$$|\psi'\rangle = |0_L\rangle\langle 0_L|\psi\rangle$$

Codewords for the 5-qubit code:

$$|0_L\rangle\langle 0_L| = \frac{1}{2}(I+G_1)\,\frac{1}{2}(I+G_2)\,\frac{1}{2}(I+G_3)\,\frac{1}{2}(I+G_4)\,\frac{1}{2}(I+Z_L)$$

Take $|\psi\rangle = |00000\rangle$.

$$|\psi'\rangle = |0_L\rangle\langle 0_L|\psi\rangle$$

$Z^{\otimes 5}$

$$= \frac{1}{2}(I+G_1)\,\frac{1}{2}(I+G_2)\,\frac{1}{2}(I+G_3)\,\frac{1}{2}(I+G_4)\,\frac{1}{2}(I+Z_L)\,|00000\rangle$$

Codewords for the 5-qubit code:

$$|0_L\rangle\langle 0_L| = \tfrac{1}{2}(I+G_1)\,\tfrac{1}{2}(I+G_2)\,\tfrac{1}{2}(I+G_3)\,\tfrac{1}{2}(I+G_4)\,\tfrac{1}{2}(I+Z_L)$$

Take $|\psi\rangle = |00000\rangle$.

$$|\psi'\rangle = |0_L\rangle\langle 0_L|\psi\rangle$$

$ZXIXZ$ $\quad$ $Z^{\otimes 5}$

$$= \tfrac{1}{2}(I+G_1)\,\tfrac{1}{2}(I+G_2)\,\tfrac{1}{2}(I+G_3)\,\tfrac{1}{2}(I+G_4)\,\tfrac{1}{2}(I+Z_L)\,|00000\rangle$$

$$= \tfrac{1}{2}(I+G_1)\,\tfrac{1}{2}(I+G_2)\,\tfrac{1}{2}(I+G_3)\,\tfrac{1}{2}(I+G_4)\,|00000\rangle$$

Codewords for the 5-qubit code:

$$|0_L\rangle\langle 0_L| = \tfrac{1}{2}(I+G_1)\,\tfrac{1}{2}(I+G_2)\,\tfrac{1}{2}(I+G_3)\,\tfrac{1}{2}(I+G_4)\,\tfrac{1}{2}(I+Z_L)$$

Take $|\psi\rangle = |00000\rangle$.

$XIXZZ$ $\quad$ $ZXIXZ$ $\quad$ $Z^{\otimes 5}$

$$\begin{aligned}
|\psi'\rangle &= |0_L\rangle\langle 0_L|\psi\rangle \\
&= \tfrac{1}{2}(I+G_1)\,\tfrac{1}{2}(I+G_2)\,\tfrac{1}{2}(I+G_3)\,\tfrac{1}{2}(I+G_4)\,\tfrac{1}{2}(I+Z_L)\,|00000\rangle \\
&= \tfrac{1}{2}(I+G_1)\,\tfrac{1}{2}(I+G_2)\,\tfrac{1}{2}(I+G_3)\,\tfrac{1}{2}(I+G_4)\,|00000\rangle \\
&= \tfrac{1}{16}(I+G_1)(I+G_2)(I+G_3)\big(|00000\rangle + |01010\rangle\big)
\end{aligned}$$

Codewords for the 5-qubit code:

$$|0_L\rangle\langle 0_L| = \tfrac{1}{2}(I+G_1)\,\tfrac{1}{2}(I+G_2)\,\tfrac{1}{2}(I+G_3)\,\tfrac{1}{2}(I+G_4)\,\tfrac{1}{2}(I+Z_L)$$

Take $|\psi\rangle = |00000\rangle$.

$XIXZZ$ $\quad$ $ZXIXZ$ $\quad$ $Z^{\otimes 5}$

$$|\psi'\rangle = |0_L\rangle\langle 0_L|\psi\rangle$$

$$= \tfrac{1}{2}(I+G_1)\,\tfrac{1}{2}(I+G_2)\,\tfrac{1}{2}(I+G_3)\,\tfrac{1}{2}(I+G_4)\,\tfrac{1}{2}(I+Z_L)\,|00000\rangle$$

$$= \tfrac{1}{2}(I+G_1)\,\tfrac{1}{2}(I+G_2)\,\tfrac{1}{2}(I+G_3)\,\tfrac{1}{2}(I+G_4)\,|00000\rangle$$

$$= \tfrac{1}{16}(I+G_1)(I+G_2)(I+G_3)\big(|00000\rangle + |01010\rangle\big)$$

$$= \tfrac{1}{16}(I+G_1)(I+G_2)\big(|00000\rangle + |01010\rangle + |10100\rangle - |11110\rangle\big)$$

$XZZXI$ $\quad$ $IXZZX$

Codewords for the 5-qubit code:

$$|0_L\rangle\langle 0_L| = \tfrac{1}{2}(I+G_1)\,\tfrac{1}{2}(I+G_2)\,\tfrac{1}{2}(I+G_3)\,\tfrac{1}{2}(I+G_4)\,\tfrac{1}{2}(I+Z_L)$$

Take $|\psi\rangle = |00000\rangle$.

XIXZZ   ZXIXZ $Z^{\otimes 5}$

$$|\psi'\rangle = |0_L\rangle\langle 0_L|\psi\rangle$$

$$= \tfrac{1}{2}(I+G_1)\,\tfrac{1}{2}(I+G_2)\,\tfrac{1}{2}(I+G_3)\,\tfrac{1}{2}(I+G_4)\,\tfrac{1}{2}(I+Z_L)\,|00000\rangle$$

$$= \tfrac{1}{2}(I+G_1)\,\tfrac{1}{2}(I+G_2)\,\tfrac{1}{2}(I+G_3)\,\tfrac{1}{2}(I+G_4)\,|00000\rangle$$

$$= \tfrac{1}{16}(I+G_1)(I+G_2)(I+G_3)\big(|00000\rangle + |01010\rangle\big)$$

$$= \tfrac{1}{16}(I+G_1)(I+G_2)\big(|00000\rangle + |01010\rangle + |10100\rangle - |11110\rangle\big)$$

XZZXI   IXZZX

$$= \tfrac{1}{16}\big(|00000\rangle + |01010\rangle + |10100\rangle - |11110\rangle\big)$$
$$\big(|01001\rangle - |00011\rangle - |11101\rangle - |10111\rangle\big)$$
$$\big(|10010\rangle - |11000\rangle - |00110\rangle - |01100\rangle\big)$$
$$\big(-|11011\rangle - |10001\rangle - |01111\rangle + |00101\rangle\big)$$

$$|0_L\rangle = \frac{|\psi'\rangle}{\||\psi'\rangle\|} = \frac{1}{\underset{4}{\cancel{16}}}\Big(|00000\rangle + |01010\rangle + |10100\rangle - |11110\rangle$$

$$|01001\rangle - |00011\rangle - |11101\rangle - |10111\rangle$$

$$|10010\rangle - |11000\rangle - |00110\rangle - |01100\rangle$$

$$-|11011\rangle - |10001\rangle - |01111\rangle + |00101\rangle\Big)$$

$$
\begin{aligned}
|0_L\rangle = \frac{|\psi'\rangle}{\||\psi'\rangle\|} = \frac{1}{\cancel{16}\ 4} \big(&|00000\rangle + |01010\rangle + |10100\rangle - |11110\rangle \\
&|01001\rangle - |00011\rangle - |11101\rangle - |10111\rangle \\
&|10010\rangle - |11000\rangle - |00110\rangle - |01100\rangle \\
&- |11011\rangle - |10001\rangle - |01111\rangle + |00101\rangle \big)
\end{aligned}
$$

$$
\begin{aligned}
|1_L\rangle = X_L |0_L\rangle = \frac{1}{4} \big(&|11111\rangle + |10101\rangle + |01011\rangle - |00001\rangle \\
&|10110\rangle - |11100\rangle - |00010\rangle - |01000\rangle \\
&|01101\rangle - |00111\rangle - |11001\rangle - |10011\rangle \\
&- |00100\rangle - |01110\rangle - |10000\rangle + |11010\rangle \big)
\end{aligned}
$$

$XXXXX$

$$|0_L\rangle = \frac{|\psi'\rangle}{\||\psi'\rangle\|} = \frac{1}{\underset{4}{\cancel{16}}}\big(|00000\rangle + |01010\rangle + |10100\rangle - |11110\rangle$$

$$|01001\rangle - |00011\rangle - |11101\rangle - |10111\rangle$$

$$|10010\rangle - |11000\rangle - |00110\rangle - |01100\rangle$$

$$-|11011\rangle - |10001\rangle - |01111\rangle + |00101\rangle\big)$$

$$|1_L\rangle = X_L|0_L\rangle = \frac{1}{4}\big(|11111\rangle + |10101\rangle + |01011\rangle - |00001\rangle$$

$$|10110\rangle - |11100\rangle - |00010\rangle - |01000\rangle$$

$$|01101\rangle - |00111\rangle - |11001\rangle - |10011\rangle$$

$$-|00100\rangle - |01110\rangle - |10000\rangle + |11010\rangle\big)$$

$$X_L = XXXXX$$

Historical note: the 5-bit code was found numerically without a derivation. The stabilizer formalism provides a possible derivation and understanding of how the code works.

9. Combating noise: quantum error correcting codes

(NC 10.1-10.3, 10.5, M 5, KLM 10)

(a) Classical noise model

(b) 3-bit repetition code

(c) Quantum noise model

(d) Quantum 3-bit repetition code for X errors

(e) Shor 9-bit code for arbitrary Pauli error

(g) Discretization and sufficient conditions for QECC

(h) Stabilizer formalism -- quantum parity checks !

5-bit code

(i) Shor 9-bit code reloaded

(j) Sufficient conditions for QECC for stabilizer codes

(l) 7-bit Steane code (later)

(m) Erasure errors, q secret sharing, AdS/CFT corr

We have understood how to correct Pauli errors.

Is it easier or harder to correct erasure errors, compared to unknown Pauli errors?

We have understood how to correct Pauli errors.

Is it easier or harder to correct erasure errors, compared to unknown Pauli errors?

Question:
if a QECC can correct up to t unknown Pauli errors, can it correct:

(a) more than t erasures
(b) t erasures
(c) fewer then t erasures
(d) nothing of the above, depends on the code

Checking our intuition in the classical setting:

For the 3-bit repetition code: 0 -> 000, 1 -> 111

- 2 unknown bit-flips (to bits 1,2) cause a logical error

  000 -> 110 -> 111

  111 -> 001 -> 000

  syndrome +-, correction flips the 3rd bit.

Checking our intuition in the classical setting:

For the 3-bit repetition code: 0 -> 000, 1 -> 111

- 2 unknown bit-flips (to bits 1,2) cause a logical error

  000 -> 110 -> 111
  111 -> 001 -> 000

  syndrome +-, correction flips the 3rd bit.

- 2 erasure (known) (to bits 1,2) can be corrected:

  000 -> EE0 -> 000
  111 -> EE1 -> 111

  by using the 3rd (trusted) bit.

Lemma: suppose a QECC can correct up to any t-qubit unknown errors, then it corrects up to 2t erasure errors!

Lemma: suppose a QECC can correct up to any t-qubit unknown errors, then it corrects up to 2t erasure errors!

NB. The lemma holds for QECC on any dim. For simplicity, d=2. Let P = projector onto C. The code corrects t unknown Pauli errors.

We will see 1 proof, and a 2nd proof is provided in the notes as reading exercise.

Proof 1: decoding procedure

1. record the 2t erasure locations.

Proof 1: decoding procedure

1. record the 2t erasure locations.

2. replace the erasure symbols by any state eg $|0\rangle^{\otimes 2t}$

Proof 1: decoding procedure

1. record the 2t erasure locations.
2. replace the erasure symbols by any state eg $|0\rangle^{\otimes 2t}$
3. those 2t qubits are evolved by a quantum operation, with Kraus operators in the span of Pauli matrices acting on those 2t qubits.

Proof 1: decoding procedure

1. record the 2t erasure locations.
2. replace the erasure symbols by any state eg $|0\rangle^{\otimes 2t}$
3. those 2t qubits are evolved by a quantum operation, with Kraus operators in the span of Pauli matrices acting on those 2t qubits.
4. by discretization, suffices to distinguish what Pauli error occurs on those 2t locations.

Proof 1: decoding procedure

1. record the 2t erasure locations.
2. replace the erasure symbols by any state eg $|0\rangle^{\otimes 2t}$
3. those 2t qubits are evolved by a quantum operation, with Kraus operators in the span of Pauli matrices acting on those 2t qubits.
4. by discretization, suffices to distinguish what Pauli error occurs on those 2t locations.

Let $\{F_i\}$ denote these Pauli errors. To see that $F_i P F_i^\dagger$'s are orthogonal projectors:

$$\forall \; i \neq j, \quad F_i P F_i \, F_j P F_j = F_i P E_a E_b P F_j$$

Proof 1: decoding procedure

1. record the 2t erasure locations.
2. replace the erasure symbols by any state eg $|0\rangle^{\otimes 2t}$
3. those 2t qubits are evolved by a quantum operation, with Kraus operators in the span of Pauli matrices acting on those 2t qubits.
4. by discretization, suffices to distinguish what Pauli error occurs on those 2t locations.

Let $\{F_i\}$ denote these Pauli errors. To see that $F_i P F_i^\dagger$'s are orthogonal projectors:

$$\forall\ i \neq j, \quad F_i P \underbrace{F_i F_j} P F_j = F_i P E_a E_b P F_j$$

Fi, Fj act nontrivially and differently on the same 2t qubits, so Fi Fj = Ea Eb, each of Ea, Eb acts nontrivially on at most t qubits, and $E_a \neq E_b$.

Proof 1: decoding procedure

1. record the 2t erasure locations.
2. replace the erasure symbols by any state eg $|0\rangle^{\otimes 2t}$
3. those 2t qubits are evolved by a quantum operation, with Kraus operators in the span of Pauli matrices acting on those 2t qubits.
4. by discretization, suffices to distinguish what Pauli error occurs on those 2t locations.

Let $\{F_i\}$ denote these Pauli errors. To see that $F_i P F_i^\dagger$'s are orthogonal projectors:

$$\forall\ i \neq j, \quad F_i P \underbrace{F_i F_j} P F_j = F_i P E_a E_b P F_j = 0$$

Fi, Fj act nontrivially and differently on the same 2t qubits, so Fi Fj = Ea Eb, each of Ea, Eb acts nontrivially on at most t qubits, and $E_a \neq E_b$.

By the QECC condition, $P E_a E_b P = 0$.

e.g. for the 5-qubit code, if the first & second qubits are erased, we have to distinguish 16 possible errors:

IIIII, XIIII, YIIII, ZIIII,
IXIII, XXIII, YXIII, ZXIII,
IYIII, XYIII, YYIII, ZYIII,
IZIII, XZIII, YZIII, ZZIII.

e.g. for the 5-qubit code, if the first & second qubits are erased, we have to distinguish 16 possible errors:

IIIII, XIIII, YIIII, ZIIII,
IXIII, XXIII, YXIII, ZXIII,
IYIII, XYIII, YYIII, ZYIII,
IZIII, XZIII, YZIII, ZZIII.

Say, if Fi = XIIII, Fj = ZYIII, Fi Fj = YYIII = (YIIII)(IYIII)
so, P Fi Fj P = P (YIIII)(IYIII) P = 0.

e.g. for the 5-qubit code, if the first & second qubits are erased, we have to distinguish 16 possible errors:

IIIII, XIIII, YIIII, ZIIII,
IXIII, XXIII, YXIII, ZXIII,
IYIII, XYIII, YYIII, ZYIII,
IZIII, XZIII, YZIII, ZZIII.

Say, if Fi = XIIII, Fj = ZYIII, Fi Fj = YYIII = (YIIII)(IYIII)
so, P Fi Fj P = P (YIIII)(IYIII) P = 0.

Therefore, the 16 projectors:

IIIII P IIIII, XIIII P XIIII, ..., ZZIII P ZZIII are orthogonal.

e.g. for the 5-qubit code, if the first & second qubits are erased, we have to distinguish 16 possible errors:

IIIII, XIIII, YIIII, ZIIII,
IXIII, XXIII, YXIII, ZXIII,
IYIII, XYIII, YYIII, ZYIII,
IZIII, XZIII, YZIII, ZZIII.

Say, if Fi = XIIII, Fj = ZYIII, Fi Fj = YYIII = (YIIII)(IYIII)
so, P Fi Fj P = P (YIIII)(IYIII) P = 0.

Therefore, the 16 projectors:

IIIII P IIIII, XIIII P XIIII, ..., ZZIII P ZZIII are orthogonal.

Once we have the syndrome, we correct the error according to the syndrome (one of the 15 two-qubit errors on the first two qubits), despite the fact it's initially an erasure.

Here, we use the erasure symbol to locate the errors, then, we modify the initial erasure to become located but unknown Pauli errors. Finally, we identify which Pauli error has occured.

Proof 2: we check that the sufficient condition for QECC is satisfied, directly for the erasure errors.

An erasure on a qubit can be described as $\mathcal{E}(\rho) = |2\rangle\langle 2|$.

In Kraus representation:

$\mathrm{tr}\,\rho = 1$

$$\mathcal{E}(\rho) = \sum_{k=0}^{1} \underbrace{|2\rangle\langle k|}_{A_k} \rho \underbrace{|k\rangle\langle 2|}_{A_k^\dagger}$$

If up to 2t erasures happen to n qubits, the quantum operation has Kraus operators of the form:

$$M_1 \otimes M_2 \otimes \cdots \otimes M_n$$

where at least (n-2t) of the Mi's equal to I, the rest are equal to $|2\rangle\langle k_1|$, $|2\rangle\langle k_2|$, ...

Consider 2 such Kraus operators E, F, and $P E^\dagger F P$.

If E, F do not have the non-identity tensor components in the same qubits, $E^\dagger F = 0$.

eg. If $E = |2\rangle\langle k| \otimes I \otimes \cdots$

$F = I \otimes I \otimes \cdots$

$I = |0\rangle\langle 0| + |1\rangle\langle 1|$, so $|k\rangle\langle 2| \cdot I = 0$, so $E^\dagger F = 0$

If $E = I \otimes I \otimes \cdots$

$F = |2\rangle\langle k| \otimes I \otimes \cdots$

similarly, $I \cdot |2\rangle\langle k| = 0$, so $E^\dagger F = 0$

So, $E^\dagger F$ has at least n-2t identity tensor factors, and up to 2t tensor factors of the form: $|k\rangle\langle 2| \cdot |2\rangle\langle \ell| = |k\rangle\langle \ell|$

If $E \neq F$, then, $E^\dagger F$ is traceless (at least one tensor component is $|k\rangle\langle \ell|$ for $k \neq \ell$).

So, $E^\dagger F$ is spanned by the 2t-qubit Pauli operators, without the identity. Since the QECC correct up to t Pauli errors, each $P E_a P = 0$ for $E_a \neq I$, E_a Pauli error on up to 2t qubits. ($\because$ $P E_i^\dagger E_j P = 0$ if E_i, E_j are at most t-qubit errors, $E_i \neq E_j$.)

$\therefore P E^\dagger F P = 0$

If E=F, $E^\dagger F$ is a tensor product of I's and $|k\rangle\langle k|$'s.

The matrix $|k\rangle\langle k| = \dfrac{I}{2} \pm \underbrace{\dfrac{Z}{2}}_{\text{traceless}}$.

The traceless part vanished in $P E^\dagger F P$. The traceful part is proportional to the identity. So, $P E^\dagger F P = mP$ where m>0.

$\square$

Remarks:

1. We do not know upfront which qubits will be erased but we know after the erasure.

Remarks:

1. We do not know upfront which qubits will be erased but we know after the erasure.

2. Erasure is related to partial trace. Ex: how are they related?

Remarks:

1. We do not know upfront which qubits will be erased but we know after the erasure.

2. Erasure is related to partial trace. Ex: how are they related?

3. Question: can the 5-qubit code correct 3 erasures ?

   (a) Yes
   (b) No

Quantum secret sharing and erasure codes

Secret sharing is a cryptographic task that encodes sensitive data into multiple quantum systems, and distribute one system to each party.

Quantum secret sharing and erasure codes

Secret sharing is a cryptographic task that encodes sensitive data into multiple quantum systems, and distribute one system to each party.

Goal: small number of malicious parties cannot collude to learn about the sensitive data or to alter it. It relies on sufficient number of honest parties.

Quantum secret sharing and erasure codes

Secret sharing is a cryptographic task that encodes sensitive data into multiple quantum systems, and distribute one system to each party.

Goal: small number of malicious parties cannot collude to learn about the sensitive data or to alter it. It relies on sufficient number of honest parties.

Simple classical example: share one bit s between 2 parties: Alice receives a, and Bob receives b.

If s=0, then ab = 00, 11 at random.

If s=1, then ab = 01, 10 at random.

Each of Alice and Bob has no information on s, but they can reconstruct s together.

Theorem (Cleve, Gottesman, Lo):

Suppose C is a QECC that encodes k qubits into n qubits, and correcting up to t erasures. If we encode a k-qubit secret into n qubits and distribute them among n parties, colluding group of up to t parties cannot learn anything about the secret, while n-t parties can jointly recover the quantum secret.

Theorem (Cleve, Gottesman, Lo):

Suppose C is a QECC that encodes k qubits into n qubits, and correcting up to t erasures. If we encode a k-qubit secret into n qubits and distribute them among n parties, colluding group of up to t parties cannot learn anything about the secret, while n-t parties can jointly recover the quantum secret.

Proof: Since the QECC corrects t erasures, n-t parties can recover the quantum secret.

Theorem (Cleve, Gottesman, Lo):

Suppose C is a QECC that encodes k qubits into n qubits, and correcting up to t erasures. If we encode a k-qubit secret into n qubits and distribute them among n parties, colluding group of up to t parties cannot learn anything about the secret, while n-t parties can jointly recover the quantum secret.

Proof: Since the QECC corrects t erasures, n-t parties can recover the quantum secret.

Conversely, suppose, by contradiction, t colluding parties can learn information about the encoded quantum secret. But the other n-t parties can decode a perfect copy of the quantum secret, violating the information gain implies disturbance principle.

NB Theorem does not hold classically.
e.g., 3 bit repetition code corrects 2 erasures, but each bit gives full information on the encoded bit.

NB Theorem does not hold classically.
e.g., 3 bit repetition code corrects 2 erasures, but each bit gives full information on the encoded bit.

Example: we can encode a secret qubit into 5 qubits, and give one qubit to each party. No two of them can learn any information about the qubit, while any 3 of them can decode the qubit.

The AdS/CFT correspondence, and modelling spacetime with holographic QECC.

quant-ph/1411.7041v3
quant-ph/1503.06237v2

https://quantumfrontiers.com/2015/03/27/quantum-gravity-from-quantum-error-correcting-codes/
(google "quantum frontiers Beni Yoshida")

https://quantumfrontiers.com/2015/03/25/putting-back-the-pieces-of-a-broken-hologram/
(google "quantum frontiers Fernando Pastawski")