Lecture III : FT Operations Part II

1

In the last lecture we covered FT error correction, state preparation & measurement.

The last class of FT operations we need to consider are logical gates.

It is not enough to protect quantum information, if we want to do FT computation we also need to process the encoded information fault-tolerantly. The most elegant way to do this is using transversal gates.

Let $\mathcal{C}$ be a QECC on n physical qubits.

Let Q_i for $i \in [m]$ $\{1, 2, \ldots, m\}$

be a partition of the physical qubits of $\mathcal{C}$ into m non-empty disjoint subsets i.e.

$$[n] = Q_1 \cup Q_2 \cup \ldots \cup Q_m$$

We say that a gate U is transversal with respect to this partition if it can be decomposed as

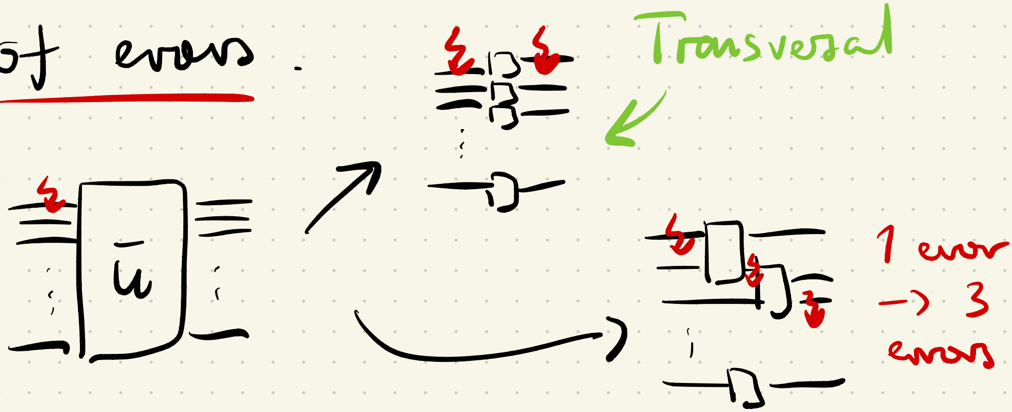
$$\mathcal{U} = \bigotimes_{i=1}^{m} U_i$$ where each unitary U_i acts only on qubits in the subset Q_i.

Most commonly, we consider the partition $Q_i = \{i\}$.

This definition also extends to gates acting on multiple code blocks or codes.

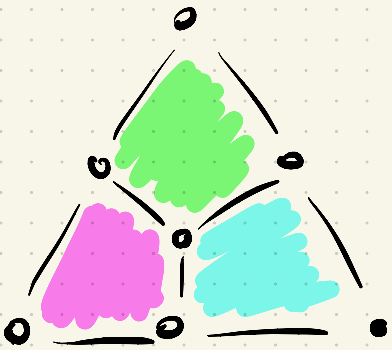
Here for two copies of a code $\mathcal{C}$ on n qubits, we often consider the partition $Q_i = \{i_A, i_B\}$ where A & B index the two code blocks.

Why do we like transversal gates? They limit the spread of errors.



Example 7 : Hadamard in the Steane code

Recall the Steane code



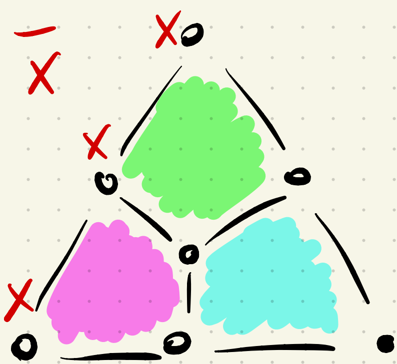
Qubits: vertices

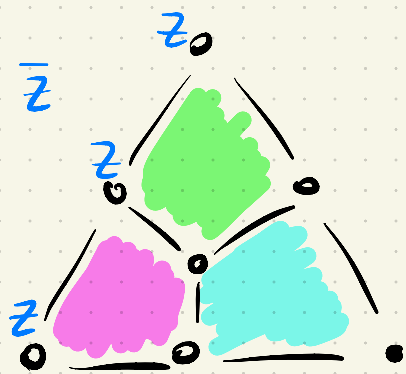
Stabilizer generators: faces

ie for each face f we have stabilizers $\prod_{v \in f} X_v$ and $\prod_{v \in f} Z_v$

where X_v denotes a Pauli X acting on the qubit on vertex v.

Logical operators





Claim : $\bar{H} = H^{\otimes 7}$

ie logical Hadamard is (single-qubit) transversal

Proof 1 : (Heisenberg picture)

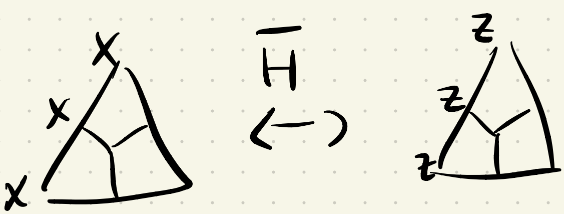
First show that it preserves stabilizer.

$$\bar{H}\left(\prod_{v \in f} X_v\right)\bar{H} = \prod_{v \in f} H X_v H$$

$$= \prod_{v \in f} Z_v$$

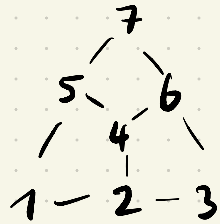
Z stabilizer

Similarly for logicals



$\square$

Proof 2: (Schrödinger picture)



$$H|0\rangle = |+\rangle$$

$$|\bar{0}\rangle = |0\rangle^{\otimes 7} + |1101100\rangle$$
$$+ |0111010\rangle + |0001111\rangle$$
$$+ |1010110\rangle + |1100011\rangle$$
$$+ |0110101\rangle + |1011001\rangle$$

$$\bar{H}|\bar{0}\rangle = |+\rangle^{\otimes 7} + |--+--++\rangle$$
$$+ |-+++-+-\rangle + \ldots$$

This is $|\bar{+}\rangle = \sum_{s \in S_Z} s|+\rangle^{\otimes 7}$

Similar argument shows $\bar{H}|1\rangle = |\bar{-}\rangle$

$\square$

Example 2

Claim: For any CSS code CNOT is transversal for 2 copies of the code.

Proof: Let A & B index the two copies.

Denote the stabilizer as

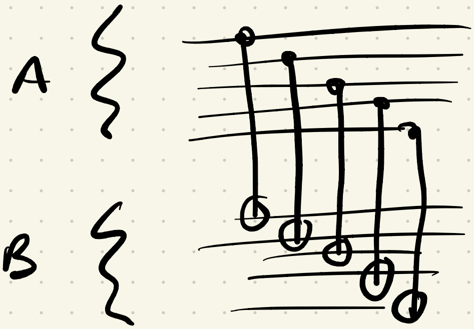
$$S = S_X \cup S_Z$$

X type operators

Z type operators

[[n,k,d]] code

$$\overline{CNOT}^{\otimes k} = CNOT^{\otimes n}$$



CNOT : $XI \to XX$

$IZ \to ZZ$

First compute action on stabilizers

For $S \in S_X$

in joint stabilizer

$$S^A \otimes I^B \xrightarrow{\overline{CNOT}} S^A \otimes S^B$$

$$I^A \otimes S^B \xrightarrow{\overline{CNOT}} I^A \otimes S^B$$

For $S \in S_Z$

$$S^A \otimes I^B \xrightarrow{\overline{CNOT}} S^A \otimes I^B$$

$$I^A \otimes S^B \xrightarrow{\overline{CNOT}} S^A \otimes S^B$$

Now let $\overline{X}_j$ be the logical X for the j'th logical qubit for $j \in [k]$

$$\overline{X}_j^A \otimes I^B \longrightarrow \overline{X}_j^A \otimes \overline{X}_j^B$$

$$I^A \otimes \overline{X}_j^B \longrightarrow I^A \otimes \overline{X}_j^B$$

This is the correct action of CNOT

Similarly

$$\bar{Z}_j^A \otimes I^B \to \bar{Z}_j^A \otimes I^B$$

$$I^A \otimes \bar{Z}_j^B \to \bar{Z}_j^A \otimes \bar{Z}_j^B \qquad \square$$

Does this mean we solved the problem of constructing fault tolerant gates?

No!

Thm [Eastin & Knill 2009]

No QECC that can correct a single erasure can have a transversal and universal set of gates.

Not enough time to prove this here. (See their original paper)

Recall: universal set of gates can approximate any unitary gate.

What does this mean?

Thm [Solovay Kitaev]

Let G be a finite subset of SU(2) containing its own inverses such that $\langle G \rangle$ is dense in $SU(d)$.

For any $\varepsilon > 0$ there exists (14)

a constant c such that for

any $U \in SU(d)$ there is a

sequence S of gates in G

of length $O(\log^c(1/\varepsilon))$ such

that $\| S - U \| \leq \varepsilon$.

$$\| S - U \| \equiv \sup_{|\psi\rangle} \| (U - S) |\psi\rangle \| \leq \varepsilon$$

$A \subseteq B$ is dense in B if the

union of A and all its limit

points is B

Informally every point in B is either in A or 'arbitrarily close' to a point in A.

Examples of universal gate sets

1. Arbitrary single qubit rotations and CNOT

Not much use to us as Eastin - Knill also rules out a code with transversal arbitrary single qubit rotations

2 Clifford + T

Very important in FT!

Recap: Clifford

gates map Pauli gates to

Pauli gates under conjugation

ie $g \in$ Clifford

iff for all Pauli gates P

$gPg^{-1} = Q$ where Q is also

a Pauli gate

Single qubit Clifford group can be generated by H & $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

Multi qubit Clifford group generated by H, S, CNOT

It's clear that H & CNOT are Clifford, but what about S?

$$SXS^{\dagger} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} & -i \\ i & \end{pmatrix}$$
$$= Y$$

$$SZS^\dagger = SS^\dagger Z = Z$$

$$SYS^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$$

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

Non-Clifford gates

$$T \text{ gate } = \sqrt{S} = \sqrt[3]{Z}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Gate set $\{H, T, \text{CNOT}\}$ universal

It is often easy to implement fault-tolerant Clifford gates in QECCs

e.g. Steane code has transversal H, CNOT & S HW!

But codes with transversal non-Clifford gates (e.g. T) are much rarer!

This will be the subject of the next lecture.

Post script

Cliffords + any non-Clifford gate is universal

[Nebe, Rains, Sloane]

Another useful universal gate set

CCZ & Hadamard

CCZ control control Z

$CCZ|111\rangle = -|111\rangle$

All other comp. basis states invariant