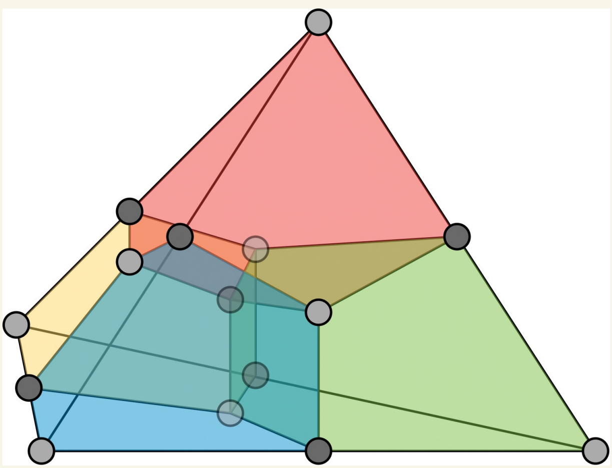
Lecture IV : Universal FT gate sets

We saw last lecture that no QECC can have a transversal universal gate set. So to construct an FT universal gate set we need to look beyond transversal gates. In this lecture we will learn how to implement an FT $\bar{T}$ gate using state injection and ②

magic state distillation.

We begin by examining a special QECC called the 15 qubit Reed-Muller code.

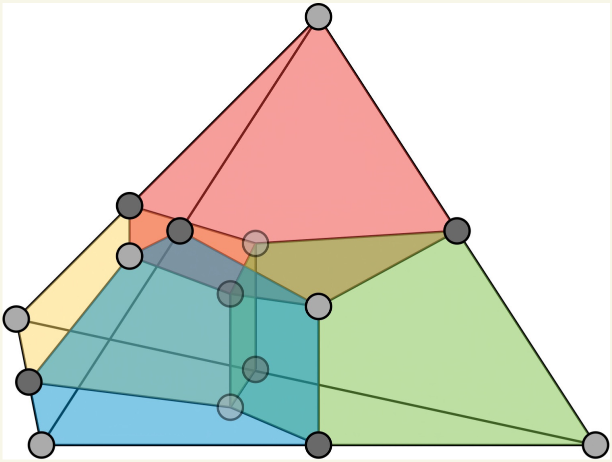
[[15, 1, 3]] code



Qubits: vertices

Z stabilizers: faces

X stabilizers: cells



For each face f we have a stabilizer generator

$$Z(f) = \prod_{v \in f} Z_v$$

Z on the qubit on v, I elsewhere

For each cell c we have a stabilizer generator

$$X(c) = \prod_{v \in c} X_v$$

Claim

The 15q RM code has a transversal $\overline{T}$ gate.

Proof

Note that $|\overline{0}\rangle$ is a superposition of Hamming weight 8 strings.

(Each S_X generator is wt 8 and generators share 4 qubits)

$\overline{X} = X^{\otimes 15}$ is a representative of logical X (easy to verify)

$\Rightarrow$ $|\bar{1}\rangle$ is a superposition of Hamming wt 7 strings.

$$T|0\rangle = |0\rangle$$

$$T|1\rangle = e^{i\pi/4}|1\rangle = \omega|1\rangle$$

$$T^\dagger|1\rangle = \omega^*|1\rangle$$

$$\bar{T} = T^{\dagger\otimes 15}$$

$$T|\bar{0}\rangle = \sum T^{\dagger\otimes 15}|\overset{\text{wt } 8}{x}\rangle$$

$$= \sum \underbrace{(\omega^*)^8}_{1}|x\rangle = |\bar{0}\rangle$$

$$T|\bar{1}\rangle = \sum_y T^{\dagger\otimes 15}|y\rangle$$

wt 7

$$= \sum_y (\omega^*)^7 |y\rangle$$

$$= \sum_y \omega |y\rangle$$

$$= \omega \sum_y |y\rangle$$

$$= \omega|\bar{1}\rangle \qquad \square$$

Codes with this property are rare and have special symmetries (triorthogonal codes).

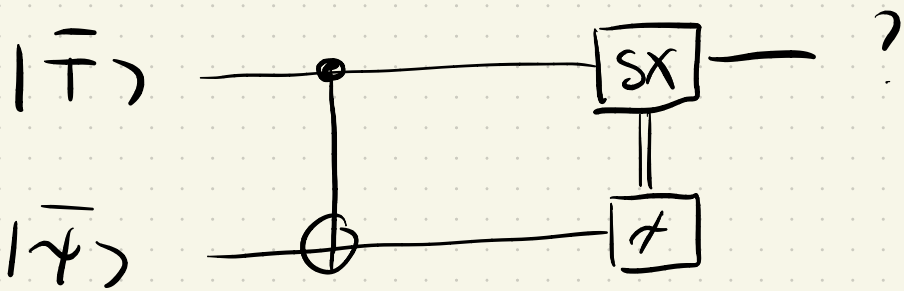
How does this help us do universal FT computation?

Suppose we start w/ the Steane code. We have transversal Clifford gates.

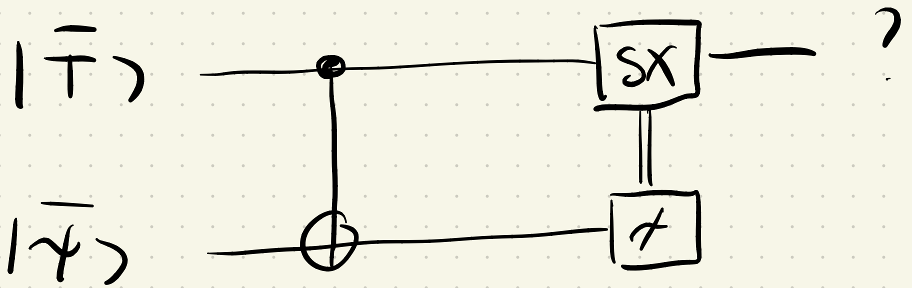
To promote this to universality we need e.g. a FT T gate.

Now suppose we can fault-tolerantly prepare the state $\bar{T}|\bar{+}\rangle = |\bar{T}\rangle$ (encoded in Steane code).

Consider



This is called a 'state injection circuit'. Let's see why.



(We drop the bars)

$$(|0\rangle + \omega|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

$$= \alpha|00\rangle + \beta|01\rangle + \omega\alpha|10\rangle + \omega\beta|11\rangle$$

$$\xrightarrow{\text{CNOT}} \alpha|00\rangle + \beta|01\rangle + \omega\alpha|11\rangle + \omega\beta|10\rangle$$

Measure q^2 :

$|0\rangle$ outcome

$$\rightarrow \alpha|0\rangle + \omega\beta|1\rangle = T|\psi\rangle$$

$|1\rangle$ outcome

$$\beta|0\rangle + \omega\alpha|1\rangle$$

$$\xrightarrow{X} \beta|1\rangle + \omega\alpha|0\rangle$$

$$\longrightarrow \omega^2\beta|1\rangle + \omega\,\alpha|0\rangle$$

$$= \omega\left[\alpha|0\rangle + \omega\beta|1\rangle\right]$$

irrelevant global phase

$$= T|+\rangle$$

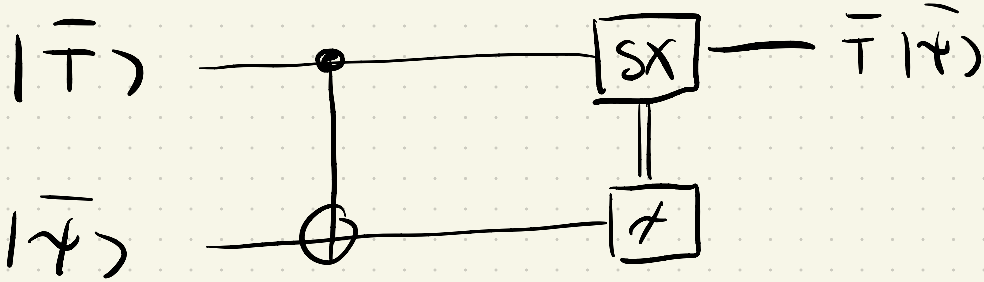
In Steane code

CNOT, X, S, Z basis meas.

are all fault-tolerant

so given $\bar{T}|\bar{+}\rangle$ we can

implement $\bar{T}$ fault-tolerantly.



Aside : To derive above circuit

commute T backwards through

teleportation circuit, see HW.

How do we prepare $T|+\rangle$?

<u>Magic state distillation</u> [Bravyi Kitaev, Knill]

Idea: start with several noisy copies of $|T\rangle = T|+\rangle$ and 'distil' them into a less noisy $|T\rangle$ state

Setup

The states

$|T\rangle = T|+\rangle$ and

$|T^c\rangle = Z|T\rangle$ form a basis for

1q states

Given an arbitrary state

$$\rho = \alpha |T\rangle\langle T| + \beta |T^c\rangle\langle T| + \gamma |T\rangle\langle T^c| + \delta |T^c\rangle\langle T^c|$$

We can apply the dephasing map

$$\mathcal{E}(\rho) = \frac{1}{2}\rho + A\rho A^{\dagger}$$

$$A = \underbrace{\omega^{*} SX}_{\text{Clifford}} = \omega^{*}\begin{pmatrix} 0 & 1 \\ \omega^{2} & 0 \end{pmatrix}$$

$$A|T\rangle = \omega^{*}\begin{pmatrix} 0 & 1 \\ \omega^{2} & 0 \end{pmatrix}\begin{pmatrix} 1 \\ \omega \end{pmatrix}$$

$$= \omega^{*}\begin{pmatrix} \omega \\ \omega^{2} \end{pmatrix} = \omega^{*}\omega\begin{pmatrix} 1 \\ \omega \end{pmatrix}$$

$$= |T\rangle$$

$$A|T^{c}\rangle = \omega^{*}\begin{pmatrix} 0 & 1 \\ \omega^{2} & 0 \end{pmatrix}\begin{pmatrix} 1 \\ -\omega \end{pmatrix}$$

$$= \omega^{*}\begin{pmatrix} -\omega \\ \omega^{2} \end{pmatrix} = -\omega^{*}\omega\begin{pmatrix} 1 \\ -\omega \end{pmatrix}$$

$$= -|T^{c}\rangle$$

Therefore, applying $\mathcal{E}$ to

$$\rho = \alpha |T X T| + \beta |T^c X T| + \gamma |T X T^c| + \delta |T^c X T^c|$$

destroys the off-diagonal elements giving

$$\rho = \alpha |T X T| + \beta |T^c X T^c|$$

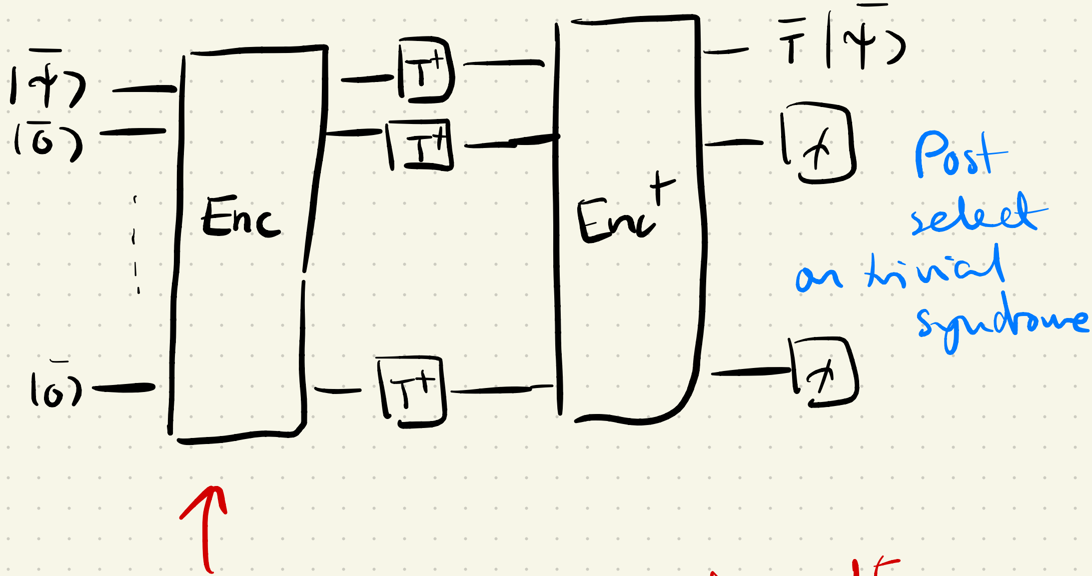
$$= (1-p) |T X T| + p |T^c X T^c|$$

We assume that we start w/ n encoded noisy $|T\rangle$ states, which we can prepare using a non FT circuit e Clifford twirling circuit

Input states

$$\rho(p) = (1-p)|\bar{T}\rangle\langle\bar{T}| + p|\bar{T}^c\rangle\langle\bar{T}^c|$$

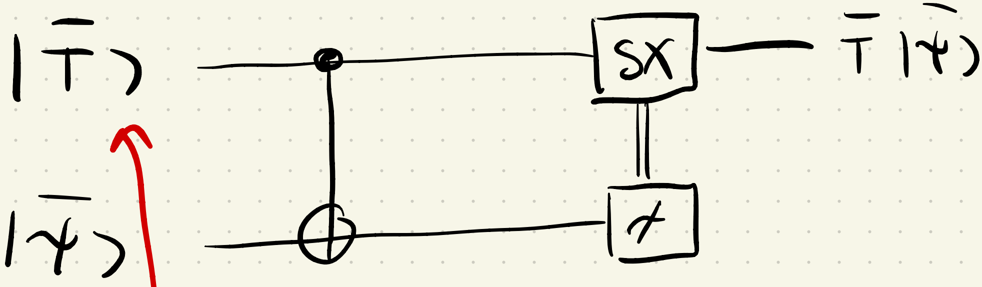
We implement the following circuit



Encoding circuit for 15q Reed-Muller code (Clifford)

We assume that the only source of error is the $T^\dagger$ gates, which we implement using our noisy T states

Recall



$$\rho(p) = (1-p)|T\rangle\langle T| + p|T^c\rangle\langle T^c|$$

The output state will be

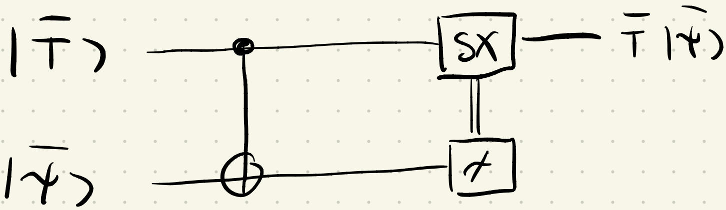
of the from

$$\rho(q) = (1-q)|T\rangle\langle T|$$
$$+ q|T^c\rangle\langle T^c|$$

We want to evaluate q

First step:

Find the probability that the syndrome is trivial



Z error on $|\bar{T}\rangle$ propagates to Z error on $\bar{T}|\bar{+}\rangle$

The syndrome will be trivial if the error commutes with the stabilizer.

$$\Pr[\text{non-trivial syndrome}]$$

$$= \sum_{E \in N_{\mathbb{P}}(S_X)} (1-p)^{15-|E|} p^{|E|}$$

Normalizer of S_X in Pauli group ie

$\{ P \in \mathbb{P} : PS = SP \ \forall S \in S_X \}$

$$= \frac{1}{|S_X|} \sum_{E \in S_X} (1-2p)^{|E|}$$ [MacWilliams identity]

$$= \frac{1}{16}\left(1 + 15(1-2p)^8\right)$$

$I \in S_X$

All other E in S_X have wt 8

Second step :

Protocol succeeds if no logical error given the syndrome was trivial

$$P[\text{success}]$$

$$= \frac{\Pr[\text{trivial syndrome } \& \text{ no logical error}]}{\Pr[\text{trivial syndrome}]}$$

$$= \frac{\Pr[\text{error is stabilizer}]}{\Pr[\text{trivial syndrome}]}$$

$$q = 1 - \frac{\displaystyle\sum_{E \in S_Z} (1-p)^{|E|} \, p^{|E|}}{\frac{1}{16}\left(1 + 15(1-2p)^{8}\right)}$$

$\vdots$ [MacWilliams]

$$= \frac{1 - 15(1-2p)^{7} + 15(1-2p)^{8} - (1-2p)^{15}}{2\left[1 + 15(1-2p)^{8}\right]}$$

$$= 35p^{3} + O(p^{4})$$

$$\Pr\left[\begin{array}{c}\text{trivial}\\ \text{synd}\end{array}\right] = 1 - 15p + O(p^{2})$$

So we started with 15 noisy $|T\rangle$ states with error p

We finish with one $|T\rangle$ state with error

$$q = 35p^3 + \mathcal{O}(p^4)$$

Now suppose we apply this procedure recursively

We have

$$q \approx 35 p^3$$

recursion level

$$P_{out}(r, p) \approx \frac{1}{\sqrt{35}} \left(\sqrt{35}\, p \right)^{3^r}$$

$15^r \approx n$ (We assume that every distillation round is successful.)

$$r \log_3(15) \approx \log_3(n) \qquad \xi = \frac{1}{\log_3(15)}$$

$$r \approx \log_3(n^\xi) \qquad \approx 0.4$$

$$3^r \approx n^\xi$$

$$P_{out}(n,p) \approx \left(\sqrt{35}\, p\right)^{n^{\xi}}$$

e.g. We want output states with error rate

$P_{out} = 10^{-10}$ given $p = \frac{1}{\sqrt{35}} 10^{-2}$

$$\log_{10}(10^{-10}) \approx n^{\xi} \log_{10}\left(\sqrt{35}\, p\right)$$

$$n \approx 5^{2.5} \approx 56$$

n is the number of encoded magic states here

So the number of physical qubits needed (assuming the logical qubits are encoded in the Steane code) is $7n$

We see that there is an overhead associated w/ magic state distillation.

Lots of subsequent reseseacrh has focussed on reducing this

Post script

There are other ways of circumventing Eastin - Knill

e.g. code switching

use two codes $\mathcal{C}_1$ & $\mathcal{C}_2$

such that the union of the transversal gates of $\mathcal{C}_1$ & $\mathcal{C}_2$ is universal

Then all we need to do is fault-tolerantly switch between $\mathcal{C}_1$ & $\mathcal{C}_2$.