FTQC Lecture Outline

What is fault-tolerant quantum computing?

- → surface code
- → threshold theorem
- → decoders for surface code
- → logical operations
- → magic state distillation

Fault-tolerant Quantum Computing

Review Quantum bit-flip code

codewords $|0\rangle_L = |000\rangle$ $\quad |1\rangle_L = |111\rangle$

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

code space $= \text{span}(\{|0\rangle_L, |1\rangle_L\}) \subset \mathbb{C}^8$
is a subspace of general 8-qubit states that represents the error free encodings

bit flip errors a bit flip on qubit 1 is, for example,

$|\psi\rangle_L \to (I \otimes X \otimes I)|\psi_L\rangle = \alpha|010\rangle + \beta|101\rangle$

error detection parity measurements $\quad Z_0 Z_1$
$\quad Z_1 Z_2$

error correction determine which X_i to apply with a "decoding algorithm." For this case this is a lookup table

logical operations i.e. doing fault-tolerant computation

$\hat{X} = X \otimes X \otimes X$ as $\quad \hat{X}|000\rangle \mapsto |111\rangle$
$\quad \hat{X}|111\rangle \mapsto |000\rangle$

$\hat{Z}|000\rangle = |000\rangle$
$\hat{Z}|111\rangle = -|111\rangle$ $\Rightarrow$ we have several choices for $\hat{Z}$ e.g.
$Z \otimes I \otimes I$ OR $I \otimes Z \otimes I$ OR $I \otimes I \otimes Z$

(Note this is not yet a universal set, we will come back to this)

Multi-qubit logical ops $\quad |\psi\rangle_L$ on a, b, c qubits
$|\varphi\rangle_L$ on a', b', c' bits

$\widehat{CNOT}(|\psi\rangle_L, |\varphi\rangle_L) = $ CNOT a a'
CNOT b b'
CNOT c c'

$\hat{X}$ and $\widehat{CNOT}$ are **transversal** e.g. you copy the physical gate to get the logical one code distance: classical = # of ops to flip code words

quantum = minimum weight of any logical operator

for $\hat{X}$ distance is 3 — can detect $(d-1)$

$\hat{Z}$ distance is 1 — can correct $(d-1)/2$

$[n,k,d]$ code is n qubit codewords w/ k encoded bits w/ distance d

$[3,1,3]$ is the bit code

Stabilizer formalism

Defines QEC's in terms of Pauli operators

Remember $P_1 = \{I, X, Y, Z\}$

$$P_N = \{ \bigotimes_j^N \sigma \mid \sigma \in P_1 \}$$ n-qubit Pauli group

$p \in P_N \Rightarrow$ $p = p^\dagger$ Hermitian, $p^\dagger = p^{-1}$ unitary

$\mathrm{eig}(p) = \{\pm 1\}$

P_N forms a basis for $2^n \times 2^n$ matrices

In the stabilizer formalism we define a quantum error correcting code by specifying its stabilizer group

Defn

Given a set of codeword basis states $|\psi_j\rangle$ on N qubits the stabilizer group is

$$S' = \{ p \in P_N \mid p|\psi_j\rangle = |\psi_j\rangle \ \forall j \}$$

i.e. all n-qubit Pauli operators that leave the codespace invariant.

$s \in S'$ is called a stabilizer operator

Corollary S' is an Abelian (commutative) subgroup of P_N.

To see that it is closed note:
$s_1, s_2 \in S' \Rightarrow s_1 s_2 \in S'$ from $s_1 s_2|\psi_j\rangle = s_1|\psi_j\rangle = |\psi_j\rangle$

To see that it is Abelian. Note that for $p, q \in P_N$ we have $pq = \pm qp$

Suppose $s_1, s_2 \in S$ and $s_1 s_2 \neq s_2 s_1$ then

$|\psi_j\rangle = s_2|\psi_j\rangle = s_1 s_2|\psi_j\rangle = -s_2 s_1|\psi_j\rangle = -s_2|\psi_j\rangle = -|\psi_j\rangle$

This is only true when $|\psi_j\rangle = \vec{0}$ vector $\Rightarrow$ contradiction $\Rightarrow$ Abelian

The stabilizer group itself is fully specified by its set of independent generators:

Thm For an Abelian group G s.t. $g \in G \Rightarrow g = g^{-1}$ then any element

$$g = \prod_j^m g_j^{a_j} \text{ where } a_j \in \{0, 1\}$$

where there are m generators and the bitstring $a_1 a_2 \ldots a_m$ describes the generating word for any given element.

Defn A set of generators is independent iff the only solution to

$$\prod_j g_j^{a_j} = I \text{ is } a_j = 0$$

This implies that a_j describes a unique element and that $|G| = 2^m$

"Analogous to linear independence"

Stabilizer example : Bit flips

Independent Generators	stabilizer group	codewords	codespace
$\{ZZI, IZZ\}$	$\left\{ \begin{matrix} ZZI \\ IZZ \\ ZIZ \\ III \end{matrix} \right\}$	$\|000\rangle$, $\|111\rangle$	$\alpha\|000\rangle + \beta\|111\rangle$

Lets check e.g. $ZZI|111\rangle = ZII(-|111\rangle) = |111\rangle$

These are the error detection measurements!

Stabilizer error detection

$s \in S'$ stabilizer operators should do nothing on the codespace, thus $\langle\psi_j|s|\psi_j\rangle = 1$.

Thus a measurement of $\langle\varphi|s|\varphi\rangle = -1$ indicates an error has occurred. (if a Pauli error then we must see it)

We only need to measure a linearly independent set of them.

For a stabilizer group s.t. $|S'| = 2^m$ w/ m generators the number of encoded logical qubits k is given by

$$k = N - m$$

where N is the number of physical qubits.

Thus a stabilizer encoding of k logical qubits from N physical ones needs only $m = n - k$ measurements (linear)

Encoded logical operations

Let $\hat{L}$ be an encoded logical operator (like $\hat{X}$ and $\hat{Z}$ from before) and $s \in \mathcal{S}$ be a stabilizer operator.

$$\hat{L}s|\psi_j\rangle = \hat{L}|\psi_j\rangle$$

We typically choose $\hat{L} \in P_N$ and in order to leave the codespace invariant $\hat{L}$ must commute w/ all s_i.

Thus the logical operators are the <u>centralizer</u> of the $\mathcal{S}$

$$\mathcal{E}(\mathcal{S}) = \{\hat{L} \in P_N \mid \hat{L}s = s\hat{L} \text{ for all } s \in \mathcal{S}\}$$

<u>Example</u> for bit flip the centralizer is

III	ZZI	ZIZ	IZZ	$\longleftrightarrow$	logical I
XXX	−YYX	−YXY	−XYY	$\longleftrightarrow$	logical X
YXX	XYX	XXY	−YYY	$\longleftrightarrow$	logical Y
ZII	IZI	IIZ	ZZZ	$\longleftrightarrow$	logical Z

confirm that the minimum weight (# of nontrivial Paulis) is 1.

<u>Ex</u> The smallest code that can correct single bit and phase flip errors is the 5 qubit code w/ $\mathcal{S}$ generators

XZZXI
IXZZX
XIXZZ
ZXIXZ

Computing codeword basis states

For example $|0_L\rangle$ is a +1 eigenstate of all stabilizers and a −1 for $\hat{Z}$ thus

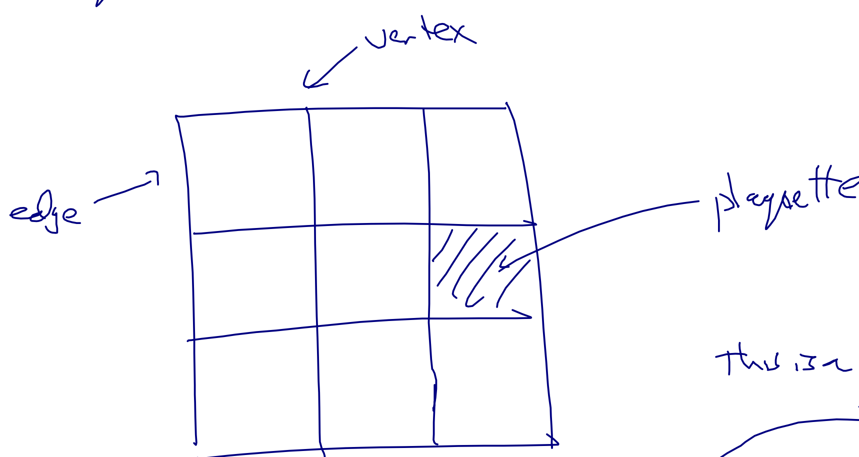
$$\rho_{0_L} = |0\rangle_L\langle 0|_L = \frac{1}{2^N}\left(1 + \hat{Z}\right)\prod_{s\in S'}(\mathbb{1} + s)$$

The rest can be constructed by logical operations

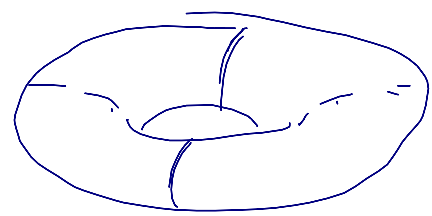
The Toric code

This is a leading plan for practical FTQC.
We use a clever topologically inspired scheme for defining stabilizers,

Consider a square lattice w/ periodic boundary conditions:



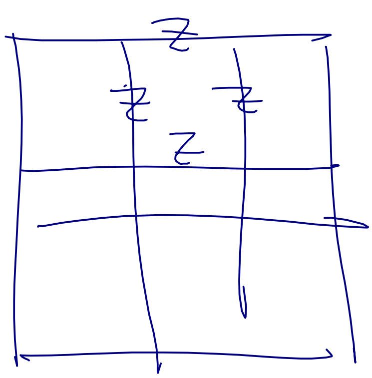
this is a torus:



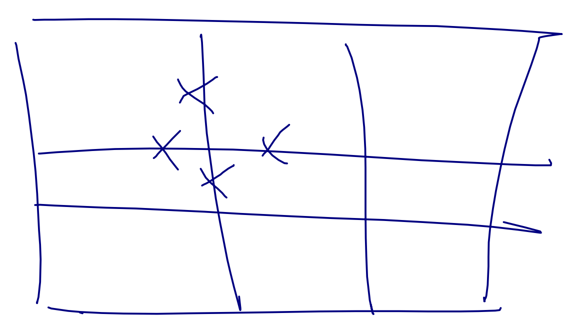
Let each edge have a qubit.
Thus an $L \times L$ lattice has

$$N = 2L^2 \text{ qubits.}$$

The toric code has two sets of generators:



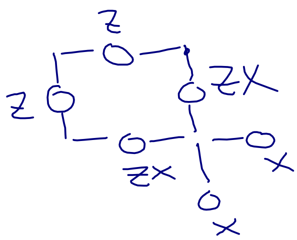
&



L^2 plaquette operators w/ Z

L^2 vertex operators w/ X

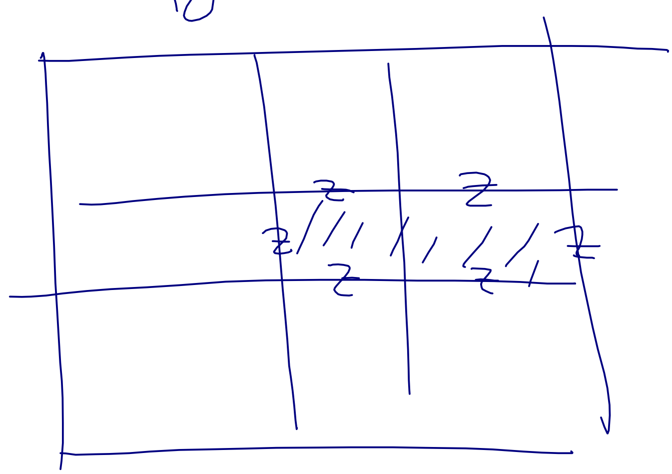
Plaquette and vertex operators commute,



as XX and ZZ commute and the overlap between any two is either weight 0 or weight 2.

Are they and independent generating set?

When we multiply them the result is the boundary e.g.



Thus periodic boundary conditions means the product of all of them is the identity so we must drop 1 plaquette to regain independence. $\Rightarrow$ L^2-1 plaquette ops

L^2-1 vertex ops

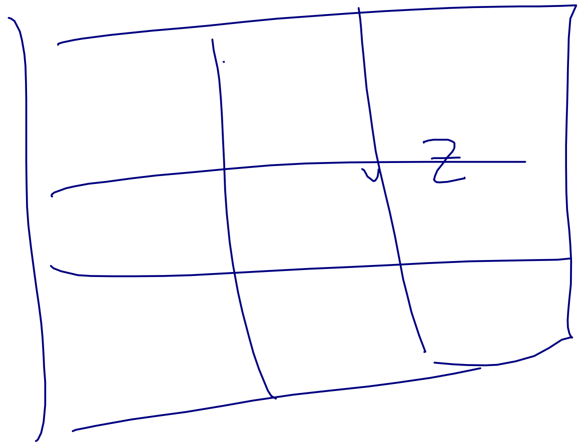
As this is a stabilizer code we know

$N-m=k \Rightarrow 2L^2-2L^2+2=k \Rightarrow k=2$ encoded qubits,

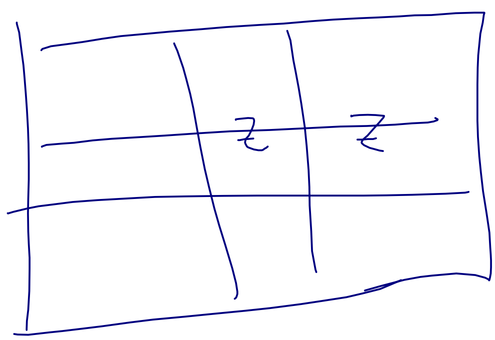
So we need logical operators $\hat{X}_1, \hat{X}_2$ and $\hat{Z}_1, \hat{Z}_2$

$\hat{Z}_1$ must commute w/ all $s \in S$ but be distinct

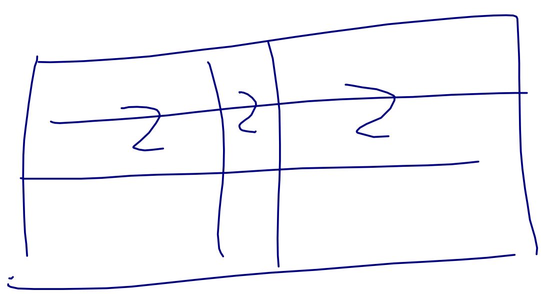
- it commutes w/ all plaquette operators
- construct



anti commutes w/ vertex v op



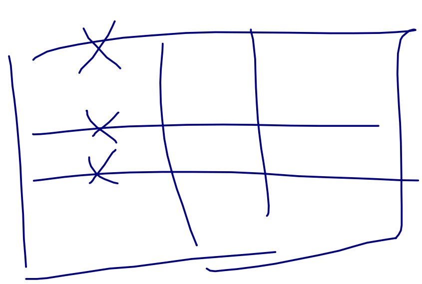
commutes but not on [illegible] ends



works! because of periodic boundries.

Closed loops on the torus generate $\hat{Z}_1$ operators.

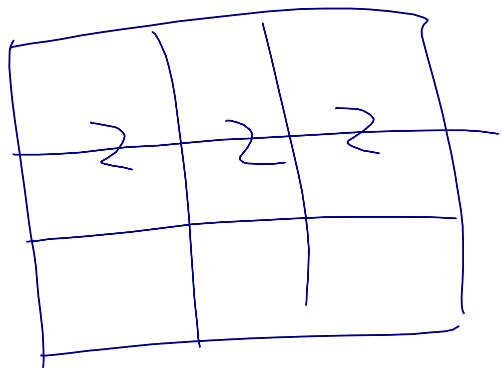
A dual argument means



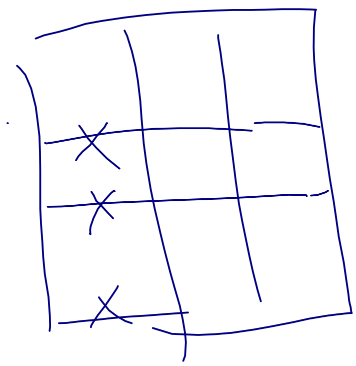
is $\hat{X}_1$

Thus

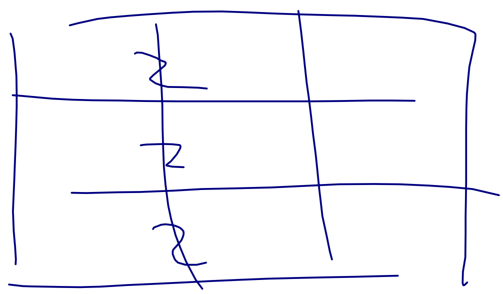
$\hat{Z}_1 =$



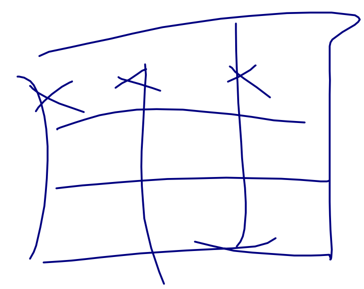
$\hat{X}_1 =$



$\hat{Z}_2 =$



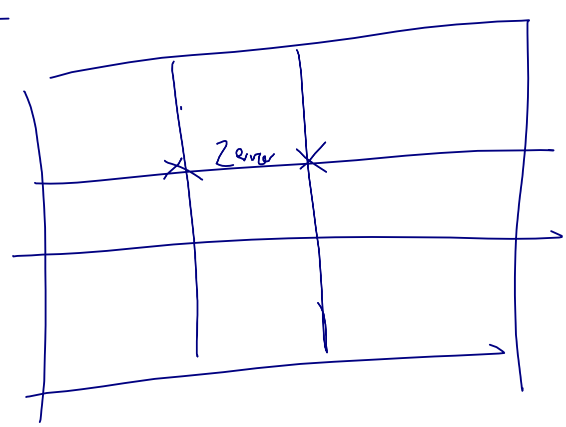
$\hat{X}_2 =$



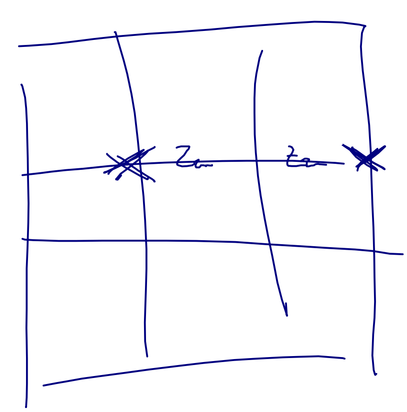
This has a high code distance for a large lattice, the minimum weight of all logical operators is L. thus the toric code is a $(n=2L^2, k=2, d=L)$ code

Error detection

example



or



The most likely correction is the minimum path between the ends.

Threshold

(1%) to 18% error rates for an uncorrelated noise model

e.g. $(1-p)^2$ = no error

$p(1-p)$ = X prob

p^2 = Y prob

$p(1-p)$ = Z prob

The code maps to an Ising model!

Universal FTQC

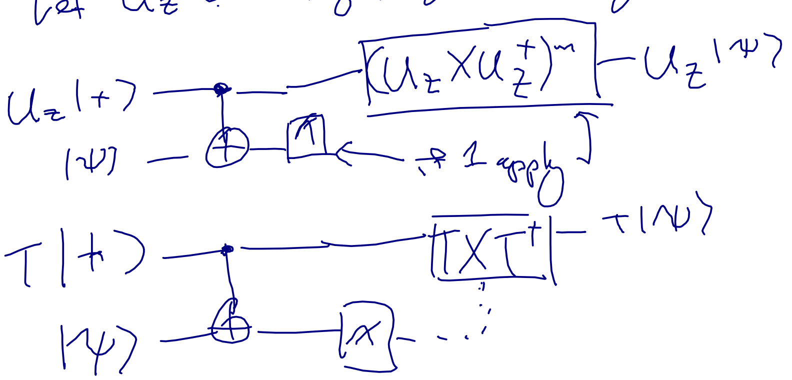
However w/ stabilizer codes give us $\hat{Z}$, $\hat{X}$ and $\widehat{CNOT}$

This is not a universal set of gates. It only gives Clifford.

However adding any other gate outside Clifford is now universal, e.g. $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

State injection

Let U_z be a single qubit unitary that commutes w/ Z



$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$

Since $TXT^\dagger = e^{-i\pi/4} YS$ we can inject T into our code.

w/ $Y, S \in$ Clifford