Meeting 9.1: Toric code

I. Kitaev's toric code

Historical note:

Toric code was introduced by Kitaev AFTER the stabiliser Formalism was developed, by Calderbank, Gottesman, Knill, Rains, Shor, Steane, et al...

Toric code is nice b/c it generalizes in different ways

i) Stabiliser codes, $\mathbb{Z}/2$ chain complexes, systolic geometry,...

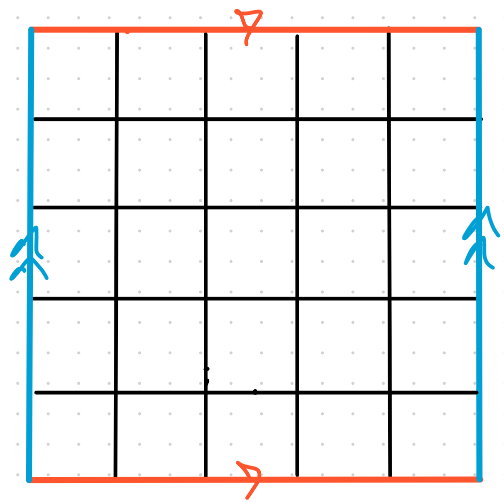
ii) other "anyonic models" (i.e. topological quantum field theory) and topological quantum computation (hardware-based approach to fault tolerance, not just error correction)

In a nutshell: stabilizer formalism is a way to convert classical linear codes over $\{0,1\}^n = \mathbb{F}_2^n$ (or other finite fields) into quantum codes. Codespace is a common eigenspace of "stabilizers", which are tensor products of X's or Z's.

More precisely: isotropic subspaces of $\mathbb{F}_2^{2n}$ w/ symplectic form correspond to stabilizer codes.

I. Toric code

Input: $n \times n$ grid on a torus



Output: A quantum code $\mathcal{H}$ with

- length $2n^2$
- distance n
- dimension 4 (two logical qubits)

Construction

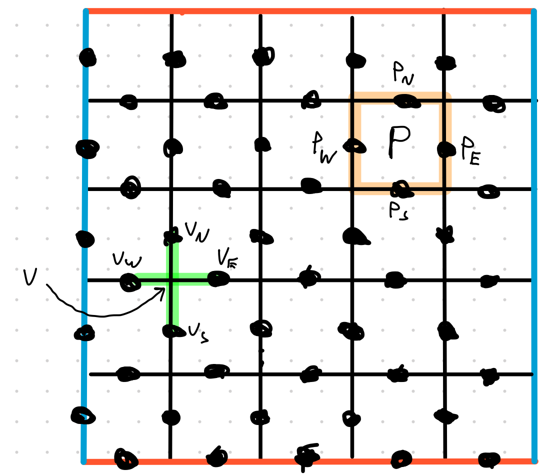
1. Put a qubit $\mathbb{C}^2$ on each edge $(2n^2)$

2. For each vertex v, define:

$$X_v = X_{v_N} X_{v_S} X_{v_E} X_{v_W}$$ (order doesn't matter)

For each 2-cell P ("plaquette"):

$$Z_P = Z_{P_N} Z_{P_S} Z_{P_E} Z_{P_W}$$ (order doesn't matter)



3. Codespace is

$$\mathcal{H} = \{ |\psi\rangle \in (\mathbb{C}^2)^{\otimes 2n^2} \mid X_v |\psi\rangle = Z_P |\psi\rangle = |\psi\rangle \ \forall P, v \}$$

So, $\mathcal{H}$ is common +1 eigenspace of all vertex and plaquette operators

<u>Claim:</u> $\dim \mathcal{H} = 4$.

<u>Proof</u>: Note all operators commute:

(justified on next page)

$$[X_{v_1}, X_{v_2}] = [Z_{p_1}, Z_{p_2}] = [X_v, Z_p] = 0.$$

So they can be simultaneously diagonalized. Note eigenvalues of X_v and Z_p are ± 1. Thus $\dim \mathcal{H} > 0$.

Also note two relations

$$\prod_v X_v = \mathrm{Id}_{(\mathbb{C}^2)^{\otimes 2n^2}} = \prod_p Z_p.$$

In fact, there are no more. (Generalities on stabilizer codes would let us stop there.)

Why is $[X_{v}, Z_p] = 0$?

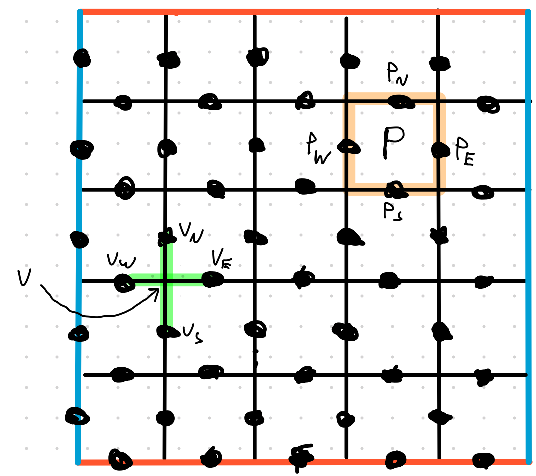
If X_v and Z_p have disjoint supports, obviously they commute

(e.g.

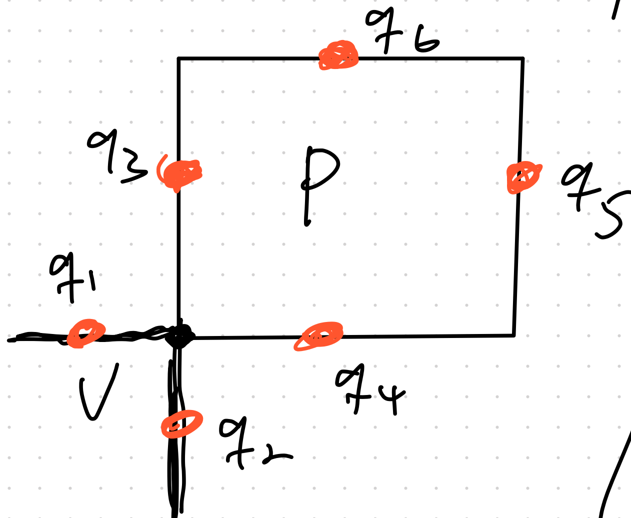
$(X \otimes 1)(1 \otimes Z)|ab\rangle$

$= (X \otimes Z)|ab\rangle$

$= (1 \otimes Z)(X \otimes 1)|ab\rangle$)



Suppose v and p overlap



$$X_v = X_1 X_2 X_3 X_4$$

$$Z_p = Z_3 Z_4 Z_5 Z_6$$

$$\begin{aligned} X_v Z_p &= X_1 X_2 X_3 X_4 Z_3 Z_4 Z_5 Z_6 \\ &= Z_5 Z_6 X_3 X_4 Z_3 Z_4 X_1 X_2 \\ &= Z_5 Z_6 X_3 Z_3 X_4 Z_4 X_1 X_2 \\ &= (-1)(-1) Z_5 Z_6 Z_3 X_3 Z_4 X_4 X_1 X_2 \\ &= Z_p X_v . \end{aligned}$$

$$\boxed{XZ = -ZX}$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Know $\mathcal{H}$ is some Hilbert space, and

$$\dim_{\mathbb{C}} \mathcal{H} = k \quad \text{if and only if} \quad \dim_{\mathbb{C}} \mathcal{B}(\mathcal{H}) \cong k^2$$

So let's compute $\mathcal{B}(\mathcal{H})$. General non-sense:

$$\mathcal{B}(\mathcal{H}) \cong \mathcal{D} / \mathcal{I}$$

where

For all v, p

$$\mathcal{D} = \{ A \in \mathcal{B}((\mathbb{C}^2)^{\otimes 2n^2}) \mid [A, X_v] = 0 = [A, Z_p] \}$$

$\mathcal{I}$ = Ideal generated by $\underset{\overset{\parallel}{X_v - \mathrm{Id}_{(\mathbb{C}^2)^{\otimes 2n^2}}}}{X_v - 1}$ and $Z_p - 1$.

Key point:

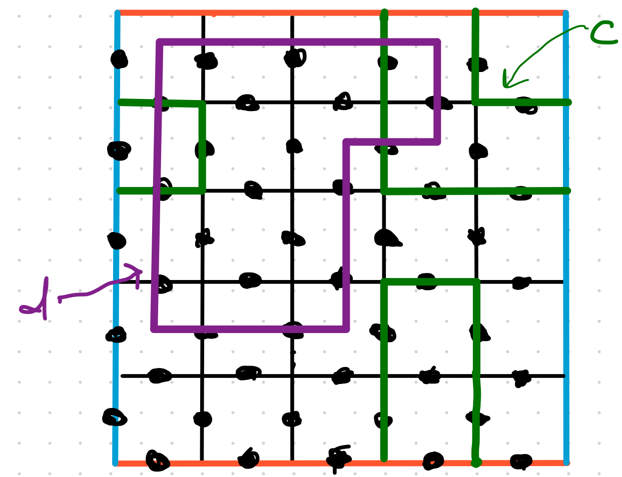
$\mathcal{D}$ has topologically meaningful generators!

If c is a loop in 1-skeleton, define

$$Z_c = \prod_{e \in c} Z_e$$

If d a loop in dual 1-skeleton, define

$$X_d = \prod_{e \in d} X_e$$



Note $Z_c, X_d \in \mathcal{G}$ for all c, d. (Why?)

Even better:

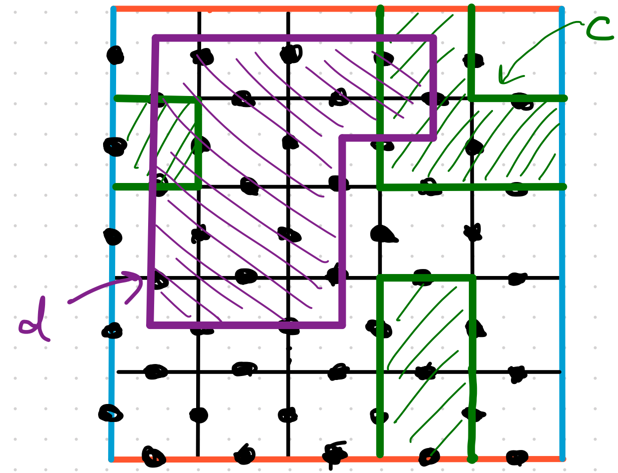
$\mathcal{G}$ is generated by Z_c and X_d.

Note, if c bounds disk D (more generally, is $\mathbb{Z}/2$-homologically trivial) then

$$Z_c = \prod_{p \in D} Z_p .$$

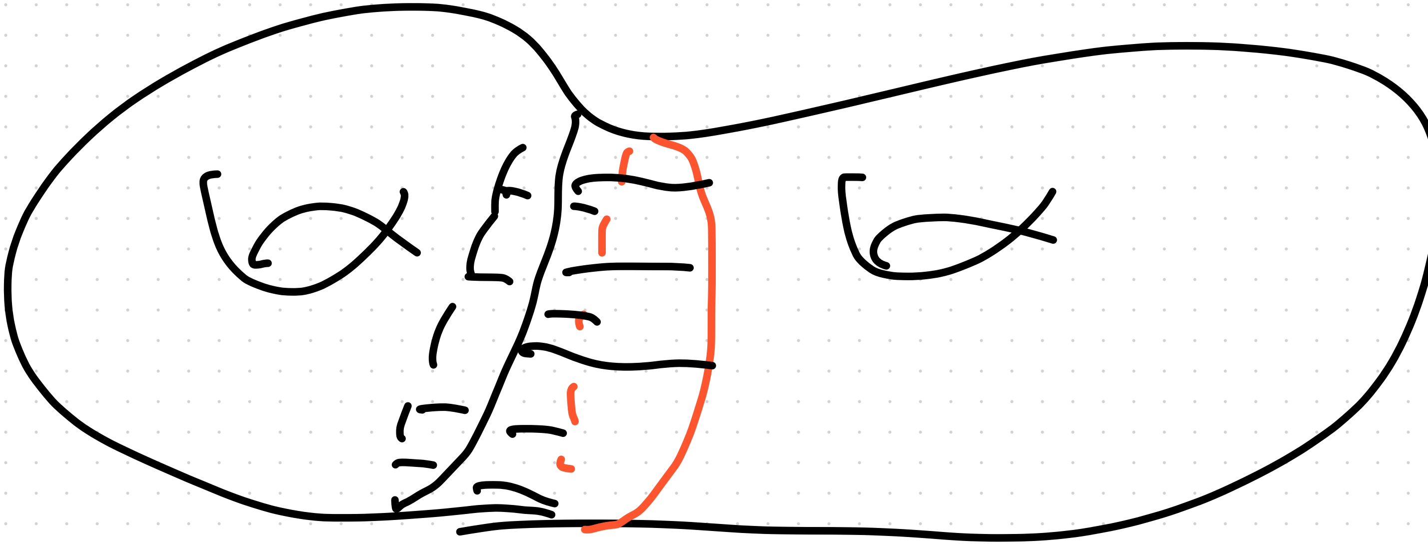
If d bounds disk D then

$$X_d = \prod_{v \in D} X_v .$$



In particular, if c and d bound, then Z_c and X_d act by identity on $\mathcal{H}$, i.e.

$$Z_c = 1 \bmod \mathcal{I} \quad \text{and} \quad X_d = 1 \bmod \mathcal{I}.$$



Corollary If $c = c'$ in $H_1(S^1 \times S^1, \mathbb{Z}/2\mathbb{Z})$, then

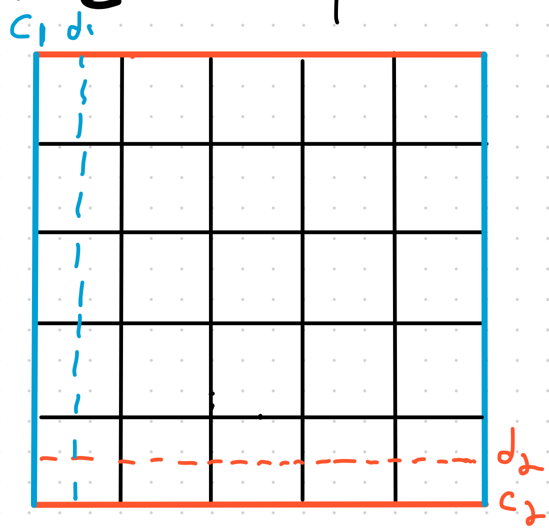
$$Z_c|_{\mathcal{H}} = Z_{c'}|_{\mathcal{H}}.$$

If $d = d'$ in $H_1(S^1 \times S^1, \mathbb{Z}/2\mathbb{Z})$, then

$$X_d|_{\mathcal{H}} = X_{d'}|_{\mathcal{H}}.$$

(Upper bounds $\dim \mathcal{B}(\mathcal{H}) \leq 16$)

Converse also true. To prove this, suffices to check that c_1, d_1, c_2, d_2 yield 16 linearly independent operators on $\mathcal{H}$.



Conclusion:

$$\dim \mathcal{B}(\mathcal{H}) = 16$$

$$\Downarrow$$

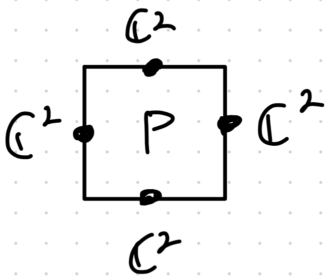
$$\dim \mathcal{H} = 4$$

What do codevectors "really" look like?

$\mathbb{C}^2 = \text{span}\{|0\rangle, |1\rangle\}$

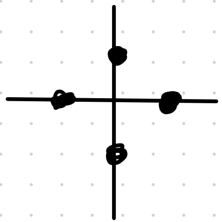
$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Suppose $|\psi\rangle \in \mathcal{H}$. Then $Z_p|\psi\rangle = |\psi\rangle \ldots$



$$Z_p|b_N b_S b_E b_W\rangle = Z_N Z_S Z_E Z_W |b_N b_S b_E b_W\rangle$$
$$= (-1)^{b_N + b_S + b_E + b_W} |b_N b_S b_E b_W\rangle$$

So, $Z_p|\psi\rangle = |\psi\rangle$ for all p means $|\psi\rangle$ must be in span of basis states where sum of bits around each P is even.



$$A_v|b_N b_S b_E b_W\rangle = |\bar{b}_N \bar{b}_S \bar{b}_E \bar{b}_W\rangle$$

Suppose $|\psi\rangle$ has some nonzero amplitude along $|b_1 b_2 \cdots b_{2n^2}\rangle$ (where $b_N + b_S + b_E + b_W = 0 \bmod 2$ for each plaquette P)

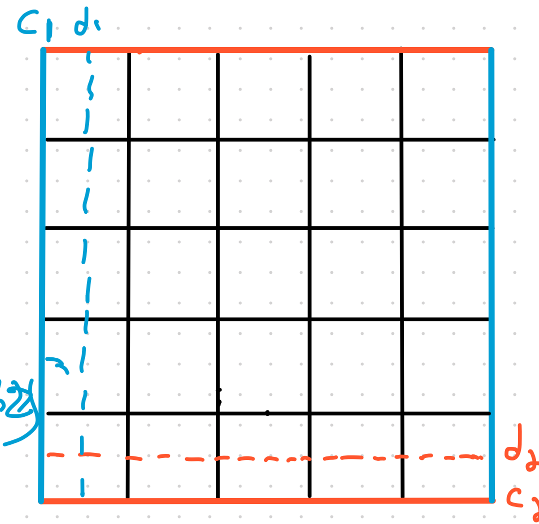
Since $A_v|\psi\rangle = |\psi\rangle$, then $|\psi\rangle$ must have same amplitude along $A_v|b_1 b_2 \cdots b_{2n^2}\rangle$.

Note: A_v preserves

$$\sum_{e \in c_1} b_e \mod 2 \quad \text{and}$$

$$\sum_{e \in c_2} b_e \mod 2.$$

"spans an element of $H_1(S^1 \times S^1, \mathbb{Z}/2\mathbb{Z})$"



Can check: if

$$\sum_{e \in c_1} b'_e = \sum_{e \in c_1} b_e \mod 2 \quad \text{and}$$

$$\sum_{e \in c_2} b'_e = \sum b_e \mod 2, \quad \text{then } \exists\, v_1, v_2, \ldots, v_\ell \text{ such that}$$

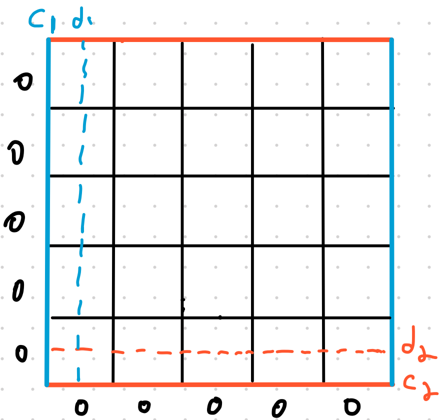
$$A_{v_1} A_{v_2} \cdots A_{v_\ell} |b_1 \cdots b_{2n^2}\rangle = |b'_1 \cdots b'_{2n^2}\rangle.$$

Note: need plaquette condition to prove it!

Conclusion: there's a basis of codevectors in bijection with elements of $H_1(S^1 \times S^1, \mathbb{Z}/2\mathbb{Z})$. More precisely, there is basis where each element is an equal superposition of all cellular representatives of given class in $\mathbb{Z}/2$ homology

E.g. $|000\cdots0\rangle$ is NOT in $\mathcal{H}$.

But it represents a $\mathbb{Z}/2$ cellular cycle (namely the 0 cycle).



Can build a code vector by summing over cellular rep's in same homology class,

$$|00\cdots0\rangle + ---$$