Lecture 2

Stabilizer codes

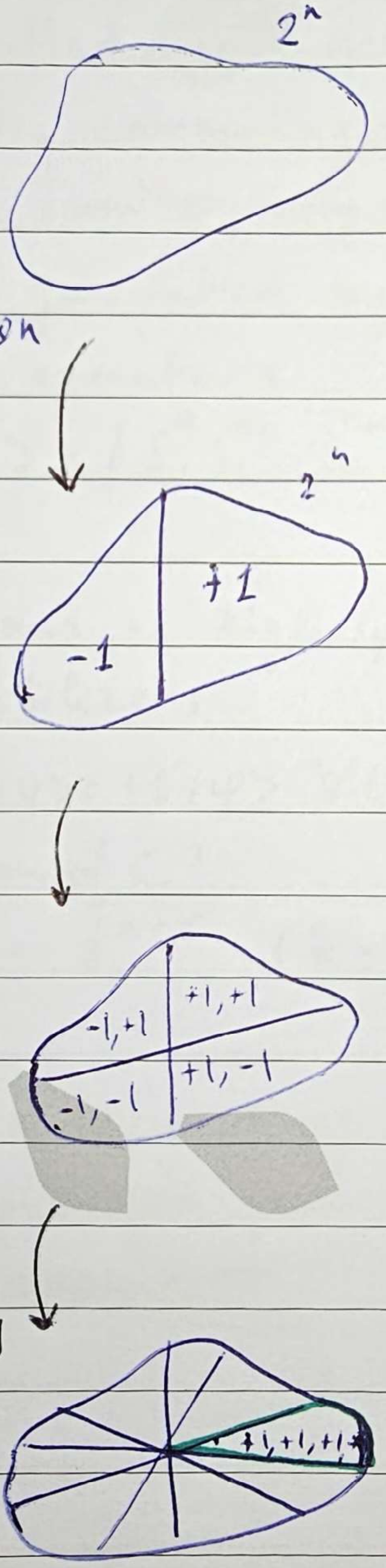
Start with n-qubit Hilbert space

Take $S_1 \in P_n = \{I, X, Y, Z\}^{\otimes n}$
(remember all Paulis have eigenvalues ± 1

S_2
$([S_2, S_1] = 0)$

...

S_r
$([S_r, S_{r-1}] = \ldots = [S_r, S_1]$
$= 0)$



Definitions :

generating set : $S_1, S_2, \ldots, S_r$

* also called check operators
* mutually commuting so they can be simultaneously measured

Stabilizer group : group generated by the check operators

$$S = \langle S_1, \ldots, S_r \rangle = \{ S_1^{a_1} S_2^{a_2} \cdots S_r^{a_r} \mid a_i \in \mathbb{Z}_2 \}$$

code space : simultaneous +1 eigenspace of the stabilizers

$$C = \{ |\psi\rangle \mid S_i |\psi\rangle = +1 |\psi\rangle \ \forall i = 1 \ldots r \}$$

What is the dimension of C?

$$\dim C = 2^{n-r} \quad (k = n-r)$$

error syndrome : the binary string of eigenvalues obtained from measuring the check operators.

Unleash ingenuity

Example: 4-qubit code $|0_L\rangle = |\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\rangle + |\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\rangle$

$|1_L\rangle = |\begin{smallmatrix}1&0\\1&0\end{smallmatrix}\rangle + |\begin{smallmatrix}0&1\\0&1\end{smallmatrix}\rangle$

* ~~What are the generators?~~ $S = \langle \begin{smallmatrix}X&X\\X&X\end{smallmatrix}, \begin{smallmatrix}Z&I\\Z&I\end{smallmatrix}, \begin{smallmatrix}I&Z\\I&Z\end{smallmatrix} \rangle$

$n=4,\ r=3 \Rightarrow k = n-r = 1$

Which generators check phase flips? $\begin{smallmatrix}X&X\\X&X\end{smallmatrix}$

* What is the syndrome of: $|\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\rangle - |\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\rangle$?

$\{-1, +1, -1\}$

$|\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\rangle$?

$\{\text{random}, +1, +1\} \xrightarrow{+1} |\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\rangle + |\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\rangle$

$\xrightarrow{-1} |\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\rangle - |\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\rangle$

* Which C is stabilized by: $S = \langle XX, ZZ \rangle$

$\rightarrow |00\rangle + |11\rangle$

$S = \langle X, Z \rangle$

$\rightarrow \{\phi\}$

the stabilizer framework gives a compact representation of C: r stabilizers must be specified instead on k states with ~~of dimension~~ 2^n terms.

What happens when an error $E \in P_n$ is applied to a stabilizer code?

1) E is a stabilizer: $E \in \langle S_1, \dots, S_n \rangle$

$\rightarrow E|\psi\rangle = |\psi\rangle \quad \forall |\psi\rangle \in C$

$\rightarrow$ E acts trivially on C

E is not an error

2) E is not a stabilizer and anticommutes with ≥ 1 stabilizer S_j: $S_j(E|\psi\rangle) = -ES_j|\psi\rangle = (-E|\psi\rangle)$

$\rightarrow E|\psi\rangle \notin C$

$\rightarrow$ E is detectable error

Are we done? Is there another option?

3) E is not a stabilizer and commutes with all stabilizers: $E \in N(S) - S$

$E|\psi\rangle \in C$

but $E|\psi\rangle \neq |\psi\rangle$

E is an undetectable error

= a logical operator

Notes: definition of distance of a quantum code:

$$d \equiv \min_{E \in N(S) - S} |E|$$

Unleash ingenuity

($|E|$ is the number of non-identity elements in E, a.k.a weight of E.)

* Error-detection criteria:

$\{E_j\}$ is a detectable set of errors iff $\forall j$

$$E_j \notin N(S) - S$$

* Error-correction (Knill-Laflamme) criteria:

$\{E_i\}$ is a correctable set of errors iff $\forall i, j$

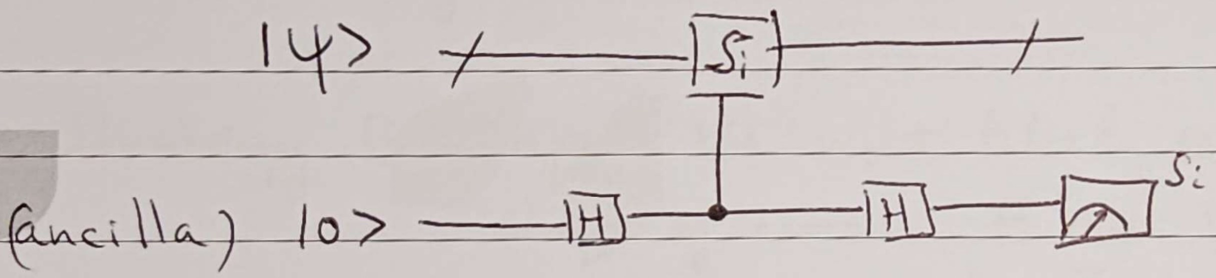
$$E_i E_j \notin N(S) - S$$

intuition: If we try to recover E_j by applying E_i (e.g. if they have equal syndrome) that should not lead to a logical error.

Unleash ingenuity

One round of QEC

① **Diagnose**: measure all stabilizer generators



HW: check that this works

$$\left(H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right)$$

→ obtain error syndrome $\bar{s} = \{s_0, \dots, s_r\}$

② **Decode**: Determine what the original logical state was

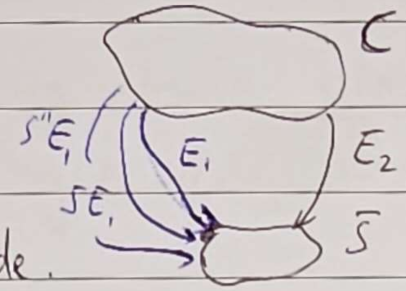
strategy A: apply the most likely error E^* consistent with $\bar{s}$

$$E^* = \underset{E \in \mathcal{P}_n}{\mathrm{Argmax}}\ \mathrm{Prob}(E \mid \bar{s})$$

This is called quantum maximum likelihood decoding (QMLD)

Is QMLD the optimal strategy?

No, one should account for all the equivalent errors in a degenerate code.



Strategy B: apply the most likely equivalence class of errors $E^* \bmod S$ consistent with $\bar{S}$.

$$E^* = \underset{E \in P_n}{\text{Argmax}} \sum_{S_i \in S} \text{Prob}(ES_i \mid \bar{S})$$

Both A&B are very hard. Lookup table impractical.

Examples: Stabilizer matrix

$$H = \begin{bmatrix} X & X & X & X \\ Z & Z & I & I \\ I & I & Z & Z \end{bmatrix}$$

What is $N(S) - S$?

$XXII = X_L$

$ZIZI = Z_L \longrightarrow$ * X_L, Z_L anticommute

* $d = \min\limits_{E \in N(S)-S} |E| = 2$

Is $\{IIII, ZIII, IIZI\}$ a corretable set?

No, $ZIII \cdot IIZI = Z_L$

and $\{ZIII, IZII, IIII\}$? Yes

CSS codes

A method for taking two classical codes for constructing a quantum code.

example: parity check matrix of

$C_x : H_x = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$

$C_z : H_z = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$

quantum code $\begin{bmatrix} X & X & X & X \\ Z & Z & I & I \\ I & I & Z & Z \end{bmatrix}$

condition $H_x H_z^T = 0 \mod 2$

What's the interpretation of this condition?

conversely, if a set of generators can be found s.t. the generators each contain only X's or Z's $\longrightarrow$ CSS code

In CSS, bit-flip and phase-flip QEC are independen

HW: understand why $d \geq \min(d_x, d_z)$

hint: $H_x (H_z^T) = 0$ and so

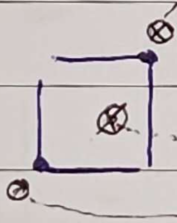
Z-stabilizers are codewords of C_x and vice-versa.

Surface code (Kitaev toric code)

Code obtained by tessellating a (2D) surface s.t.

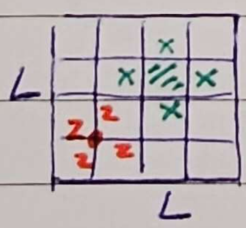
edges = qubits
faces (plaquettes) = X checks
vertices (stars) = Z checks

example:

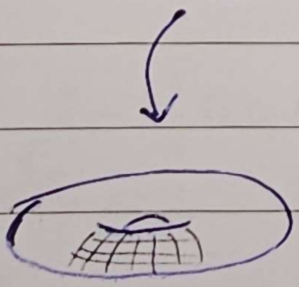


$S = \left\langle \begin{smallmatrix} X & X \\ X & X \end{smallmatrix}, \begin{smallmatrix} Z & I \\ Z & I \end{smallmatrix}, \begin{smallmatrix} I & I \\ Z & Z \end{smallmatrix} \right\rangle$

We can define a code family with increasing n by increasing lattice size.



* X and Z checks overlap on 0 or 2 qubits
→ they automatically commute.



* If we take periodic bound. conditions we get a torus.

How many logical qubits are encoded?

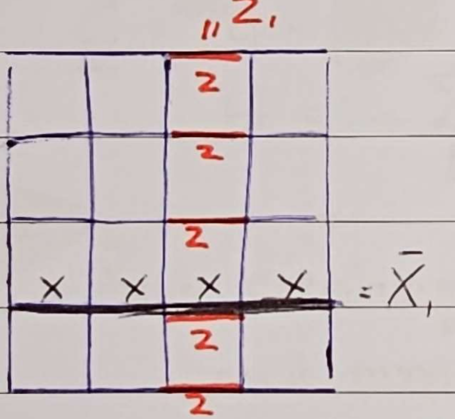
$n = L^2$

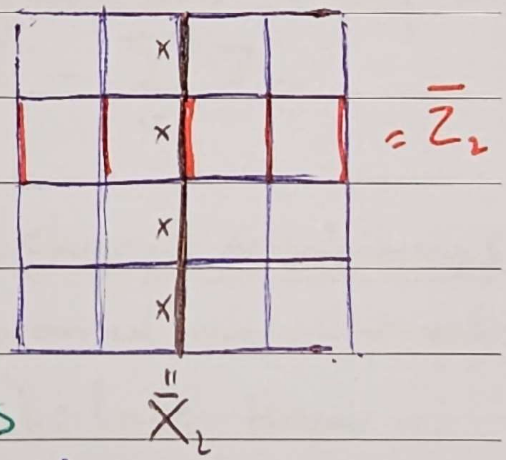
$\#\text{faces} = \#\text{vertices} = L^2$

but $\prod_v Z_v = \prod_f X_f = I$

$\Rightarrow k = n - r = L^2 - (L^2 - 2) = 2$

What are the logical operators?

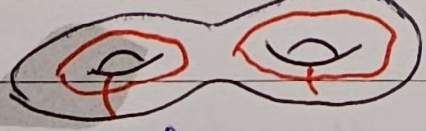




non-contractible loops

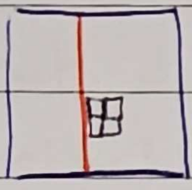
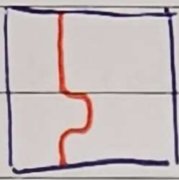
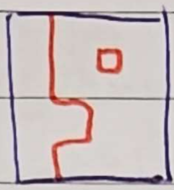
$\Rightarrow d = L$: logical information encoded in global degrees of freedom (checks & noise are local)

2D surface code is a $[[n, 2, \sqrt{n}]]$ code.



more generally, $k = 2 \times$ no. of handles $= 2g$

Note: Logical operators can be deformed using stabilizers

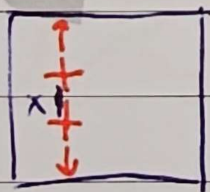
$\bar{X}_2 =$  $\underset{\text{mod } S}{=}$  $\underset{\text{mod } S}{=}$ 

<u>Condensed Matter interpretation:</u>

$\underline{C}$ = 4-fold degenerate manifold of

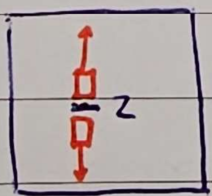
$$H = -\sum_{g} X_g - \sum_{v} Z_v$$

$\bar{X}_{1,2}$ = creating 2 <u>charge excitations</u> and moving around non-contractible loop to annihilate them



charge = vertex defect with -1 eigenvalue / energy

$\bar{Z}_{1,2}$ creating 2 fluxon excitations and annihilating across non-contractible loop



fluxon = plaquette defect with -1 eigenvalue

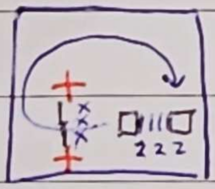
* $\prod Z_v = \prod X_f = I$

→ excitations come in pairs.

What do we get when we annihilate excitations along a contractible loop?

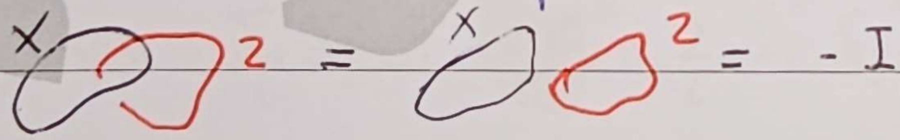
Stabilizer operation → I_L

What do we get when we encircle a fluxon with a charge?



The X and Z loops cross once → anticommute

→ -1 phase (abelian anyons)

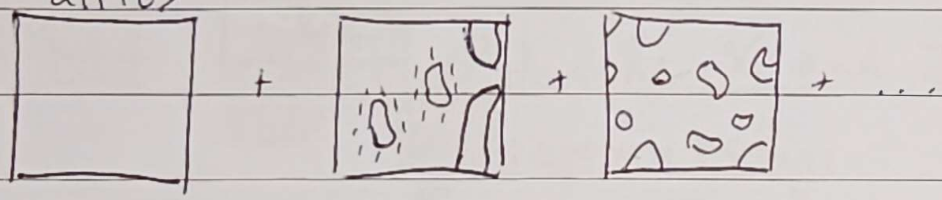


What do the logical states look like?

Take $|\varphi\rangle \equiv \sum_{S_x^i \in S_x} S_x^i \, |0\rangle^{\otimes n}$

S_x = all contractible loops of X's

all $|0\rangle$

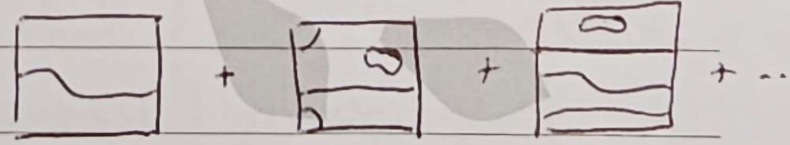


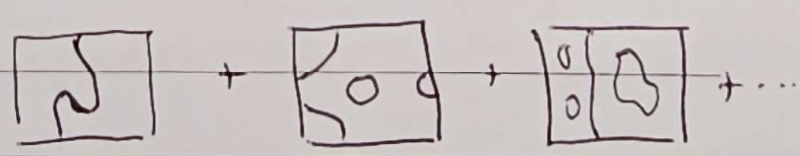
Let's check the properties of $|\varphi\rangle$:

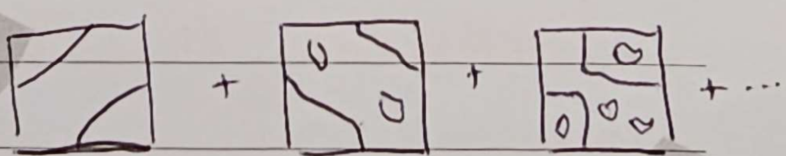
$$S_j^x |\varphi\rangle = \sum_i S_j^x S_i^x \, |0\rangle^{\otimes n} = \sum_{i'} S_{i'} \, |0\rangle^{\otimes n} = |\varphi\rangle$$

$$S_j^z |\varphi\rangle = \sum_i S_j^z S_i^x \, |0\rangle^{\otimes n} = \sum_i S_i^x S_j^z \, |0\rangle^{\otimes n} = |\varphi\rangle$$

$\Rightarrow |\varphi\rangle \in C$. Let's assign $|00\rangle_L \equiv |\varphi\rangle$

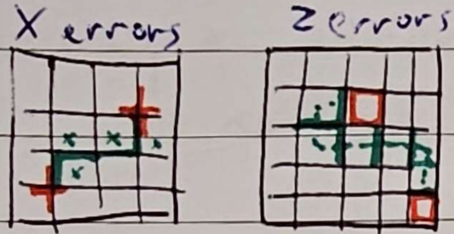
$|10\rangle_L = \bar{X}_1 |00\rangle =$ 

$|01\rangle_L = \bar{X}_2 |00\rangle =$ 

$|11\rangle = \bar{X}_1 \bar{X}_2 |00\rangle =$ 

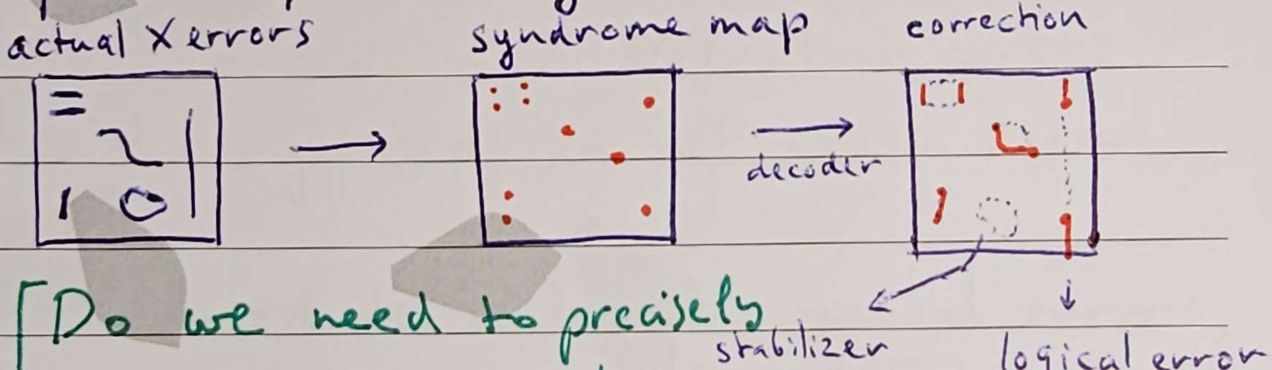
Decoding

Strings of Z/X errors are detected by face/vertex stabilizers at the endpoints



CSS code → we can decode X and Z errors separately.

problem of decoding:



[Do we need to precisely correct the original error?

Minimum Weight Perfect Matching (MWPM): efficient decoder that finds the lowest-weight (i.e. shortest) pairing of nontrivial (-1) syndromes.

Remember - MWPM is suboptimal
degeneracy needs to be taken into account.

The distance of the surface code is

$$d = \sqrt{n}$$

The probability of each single qubit having an error is p.

$\longrightarrow$ average # errors $= np$

problem: for $n > \frac{1}{p^2}$ the probability for an error with weight $> d$ tends to 1.

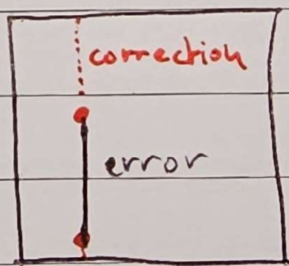
are we doomed? No! Most errors with weight $> d$ do not cause logical errors.

We need to deal with typical errors, not worst-case errors.

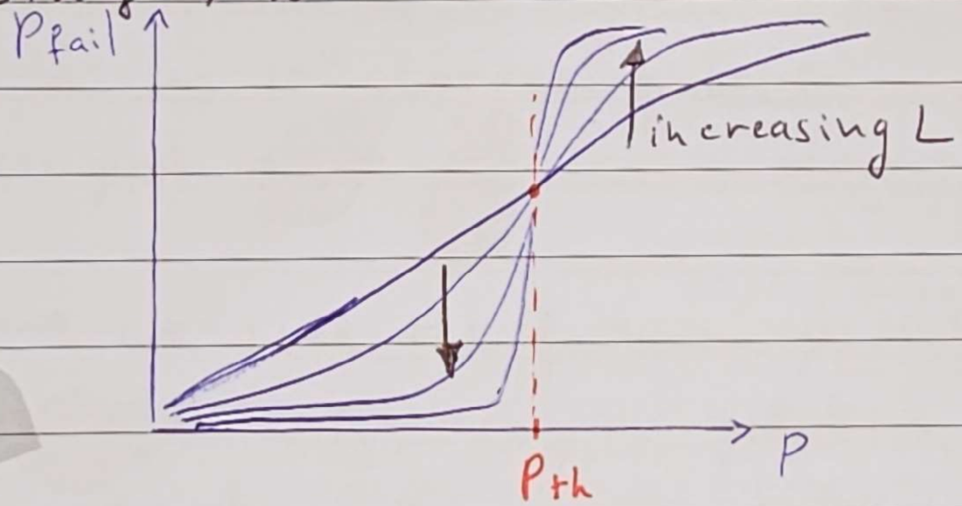
What's the probability of an error that will be incorrectly decoded?

we expect roughly:

$$p_{fail} \propto p^{\frac{d+1}{2}}$$



Let's simulate an $L \times L$ surface code under independent and identically distributed errors on each qubit $p_x = p_z = p$ using MWPM decoder.



empirical logical failure rate:

$$p_{fail} \simeq 0.03 \left(p/p_{th}\right)^{\frac{d+1}{2}}$$

with $p_{th} \sim 0.01$.

Our code + noise model + decoder has a threshold:

$\exists\, p_{th} > 0$ s.t. $p_{fail} \xrightarrow[L\to\infty]{} 0$ for $p < p_{th}$

Why is this so important? Once qubit errors are beyond threshold, scaling can arbitrarily reduce the error rate.

case study: factoring a 2048-bit integer using Shor's algorithm requires:

depth ~ 10^{10} QEC cycles (1 μs → 8 hrs)
k ~ 10^4 logical qubits
success prob. ~ 90%

→ we need the failure probability of a single logical qubit in a single QEC cycle to be:

$$p_{fail} = 0.1 \times 10^{-10} \times 10^{-4} = 10^{-15}$$

assuming physical qubit error $p \sim 0.001$ we obtain:

$$10^{-15} \approx 0.03\,(0.1)^{\frac{d+1}{2}}$$

$$\Rightarrow d \sim 27$$

So we need ~1000 qubits per logical qubit

[[1000, 1, 27]]

HW: estimate the success prob. of Shor's algo. if we use the 5-qubit code.

Threshold theorem (Aharonov, Ben-Or '97)

A circuit with k logical qubits and $T(k)$ logical gates can be computed to arbitrary accuracy ε with overhead

$$\frac{n_{TOT}}{k} = \text{polylog}\left(\frac{T(k)}{\varepsilon}\right)$$

provided the physical qubit error rate is $p < p_{th}$.

"proof" for surface code:

$$p_{fail} \simeq A \left(p/p_{th}\right)^{\sqrt{n_{TOT}/k}} \sim \varepsilon/T(k)$$

$$\left(c \equiv p/p_{th} < 1\right) \Rightarrow \sqrt{\frac{n_{tot}}{k}}\log c \sim \log\left(\frac{\varepsilon}{A\,T(k)}\right)$$

$$\Rightarrow \frac{n_{tot}}{k} \sim \left[\frac{\log\left(\frac{A\,T(k)}{\varepsilon}\right)}{\log\left(1/c\right)}\right]^2$$

Unleash ingenuity