QEC lecture

ENCCS Quantum Autumn School, Nov. 6 2025

Mats Granath

Quantum Error Correction

Stabilizer codes and decoding

Basic idea is same as for classical error correction $\Leftrightarrow$ redundancy

e.g. $0 \rightsquigarrow 000$ classically, measure each bit, correct based on majority rule

$1 \rightsquigarrow 111$

3 main obstacles

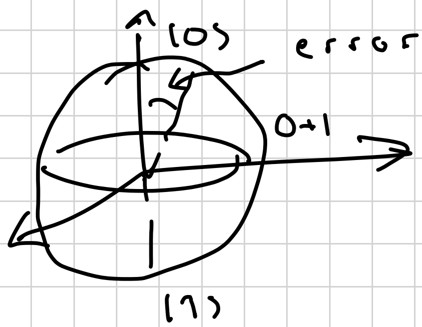
1) No cloning $\Leftrightarrow$ copy a state to several qubits?

2) Measurements are projective
$\updownarrow$
How to avoid destroying the quantumness of the state we want to protect?

3) Qubits have continuous degrees of freedom

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \ |\alpha|^2 + |\beta|^2 = 1$

i.e. infinitelly susceptible to errors?



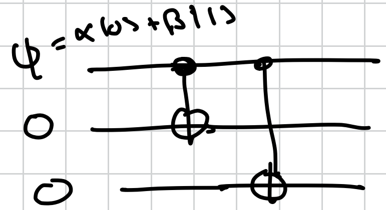
Solutions

1) Solved by encoding, not copying

$$\alpha|0\rangle + \beta|1\rangle \underset{\substack{\text{encoding}\\ \text{circuit}}}{\rightsquigarrow} \alpha|0\rangle_L + \beta|1\rangle_L$$

logical qubits

e.g.



$\alpha|000\rangle + \beta|111\rangle$

2) Do measurements that do not distinguish between logical states

3) Measurements project to discrete errors. In analogy with

$$R_x(\alpha)|0\rangle = \cos\frac{\alpha}{2}\,\mathbb{1}|0\rangle - i\sin\frac{\alpha}{2}\,X|0\rangle$$

$\rightsquigarrow$ $\mathbb{1}|0\rangle$ with prob. $\cos^2\frac{\alpha}{2}$

$X|0\rangle$ with prob $\sin^2\frac{\alpha}{2}$

here we're saved by the quantumness

Prime example of QEC codes that satisfy these constraints are

stabilizer codes

Stabilizer codes

A set of independent commuting operators

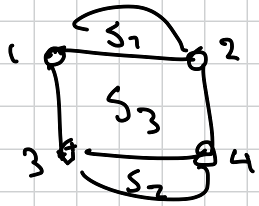
S_i $\quad$ $S_i \neq S_j S_k$ $\quad$ $[S_i, S_j] = 0 \quad i \neq j$

$i = 1, .. m$

From the Pauli group over n qubits

Example $\quad S_1 = X_1 X_2 \quad S_2 = X_3 X_4 \quad S_3 = Z_1 Z_2 Z_3 Z_4$

Quantum code
$[[n, k, d]]$



the $[[4,1,2]]$ code

nr of qubits $\quad$ nr of logical qubits $\quad$ code distance

S_i are the generators of the stabilizer group

Any product $S_i S_j$ is also a stabilizer

The point!

Define logical qubit states that are stabilized by the stab. group

$$|\psi\rangle_L : \; S_i |\psi\rangle_L = |\psi_L\rangle \quad \text{all } i$$

For the $[[4,1,2]]$ code we derive the logical states

1. $|++\rangle_{12}$ and $|--\rangle_{12}$ are stabilized by $X_1 X_2$

   $|++\rangle_{34}$ and $|--\rangle_{34}$ — " — $X_3 X_4$

2. $Z_1 Z_1 |++\rangle_{12} = |--\rangle_{12} \quad Z_1 Z_1 |--\rangle_{12} = |++\rangle_{12}$

3. Two logicals:

$$|\psi_1\rangle_L = (|+\rangle_{12} + |-\rangle_{12})(|+\rangle_{34} + |-\rangle_{34})$$

$$|\psi_2\rangle_L = (|+\rangle_{12} - |-\rangle_{12})(|+\rangle_{12} - |-\rangle_{12})$$

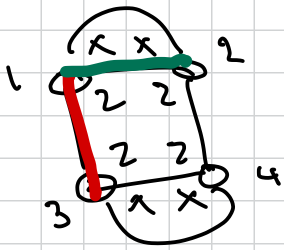
What are the logical Pauli operators X_L and Z_L? logical bit & phase flips

Need to satisfy:

1) $[X_L, S_i] = [Z_L, S_i] = 0$

because they should act within the code space = logical qubit space

2) $\{X_L, Z_L\} = X_L Z_L + Z_L X_L = 0$



Easy to construct X_L & Z_L for this code

take $\underline{X_L = X_1 X_3}$

$\underline{Z_L = Z_1 Z_2}$

Define $|0\rangle_L$: $Z_L|0\rangle_L = |0\rangle_L$

we find $|0\rangle_L = |\psi_1\rangle_L$

and $X_L|0\rangle_L = |1\rangle_L$

we find $|1\rangle_L = |\psi_2\rangle_L$

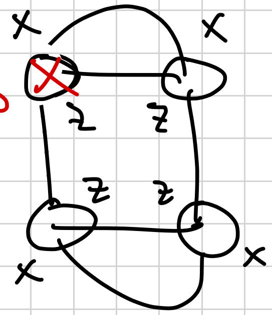
VII <u>Code distance</u>, d

Minimal weight of a logical operator

Here $\underline{\underline{d=2}}$

Can we detect and correct errors in the [[4,1,2]] code?

bit-flip error



$$|\psi\rangle_L \overset{X_1}{\rightsquigarrow} X_1|\psi\rangle_L = |\psi'\rangle$$

$$\langle\psi'|S_3|\psi'\rangle = \langle\psi_L|X_1 Z_1 Z_2 Z_3 Z_4 X_1|\psi_L\rangle$$

commute through

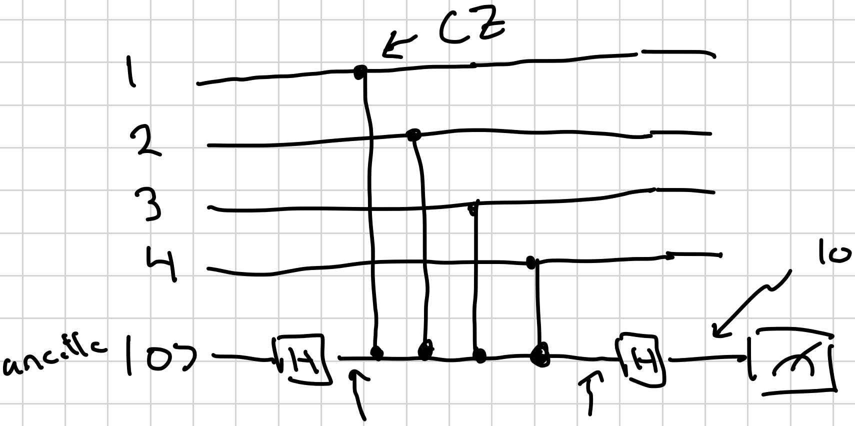
$$= -\langle\psi_L|X_1^2 S_3|\psi_L\rangle$$

$$= -1$$

$\Leftarrow$ $|\psi'\rangle$ not stabilized by S_3

S_3 detects the bitflip error

In practice we need to use an extra, ancilla/measure qubit to measure the syndrom, i.e. the set of violated stabilizers



$\Leftarrow$ measure $\rightsquigarrow$ 0 or 1

stab. ok

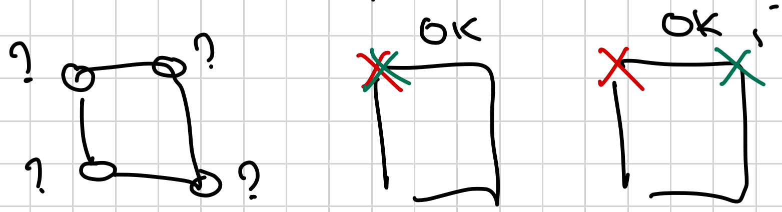
stab. violated

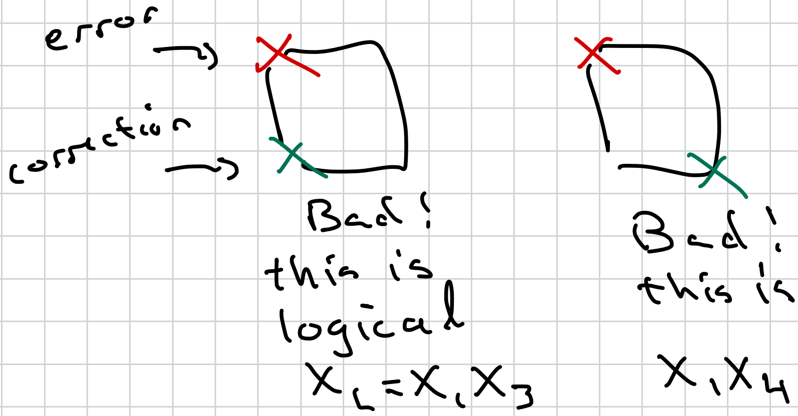
By doing the measurement the data qubit state is projected to even or odd number of bit-flips $\Rightarrow$ two bit-flip errors cannot be detected

In general a distance d code can detect $d-1$ errors.

How about correcting the X_1 error?

We only know there is an X error on one of the 4 qubits





$$X_1X_4 = X_1X_3(X_3X_4) = X_1X_3S_2 \approx X_L$$

50% chance that we do a logical bit-flip as we correct a bit-flip error

$\therefore$ We cannot correct even a single error, only detect (we could possibly post-process and throw out erroneous calculations)

☑ In general a distance d code can correct $\lfloor \frac{d-1}{2} \rfloor$ errors

Repetion code

We now consider a simpler code that can both detect and correct errors, but only of one type: X or Z errors.

It can also be scaled $\rightsquigarrow$ increase code-distance
↓
correct more errors
↓
lower *logical* error rates

The beauty of QEC $\Rightarrow$, by scaling up the code error rates can be made arbitrarily small.

Provided base error rates are below some code dependent threshold value.

aka *Threshold theorem*

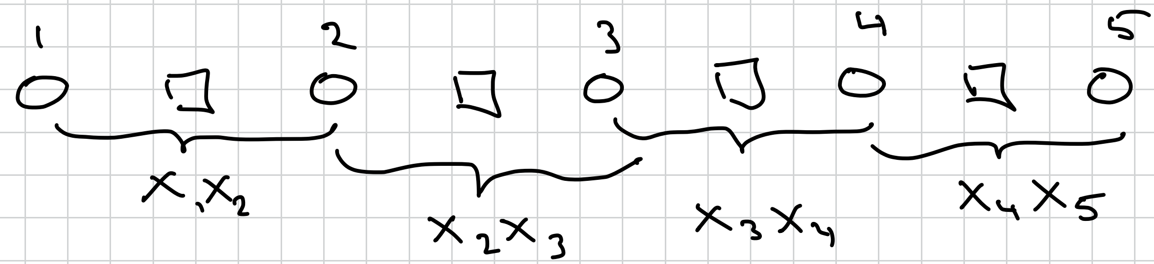
Rep. code for phase errors:

d data qubits

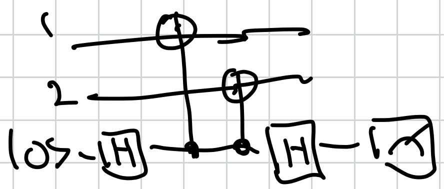
d-1 measure qubits, i.e d-1 stabilizers

$S_i = X_i X_{i+1}$

$d=5$



circuit



Stabilized states = code-words = logical states

$X_1 X_2 |++\rangle = |++\rangle$

$X_1 X_2 |--\rangle = (-1)^2 |--\rangle = |--\rangle$

same for all S_i

$\therefore |\psi_1\rangle_L = |+++++\rangle \ldots$ extended for higher d

$|\psi_2\rangle_L = |-----\rangle \ldots$

logical operators

code-distance d for Z $\rightarrow$ $X_L = Z_1 Z_2 Z_3 Z_4 Z_5$ commutes with all $S_i = X_i X_{i+1}$

code-distance 1 for X $\rightarrow$ $Z_L = X_1$ (or any other qubit)

$Z_L |\psi_1\rangle = |\psi_1\rangle \therefore |\psi_1\rangle_L = |0\rangle_L$

$Z_L |\psi_2\rangle = -|\psi_2\rangle \therefore |\psi_2\rangle_L = |1\rangle_L$

check $X_L |0\rangle_L = |1\rangle_L$ $(Z|+\rangle = |-\rangle)$

can only detect and correct Z-errors

How correct errors?

Measure a syndrome $\leftarrow$ set of violated stabilizers

$\downarrow$ $\boxed{\text{Decoder}}$

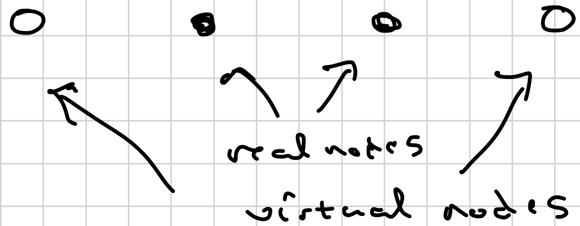
Suggest correction

Minimum Weight Perfect Matching (MWPM)

Graph algorithm that can be used for decoding. Works for "matchable" codes such as the repetion and surface code where an error is detected by two stabilizers.

Rep. code example $d=5$ (no measurement errors)

$\Downarrow$ graph with 2 nodes + + 2 virtual

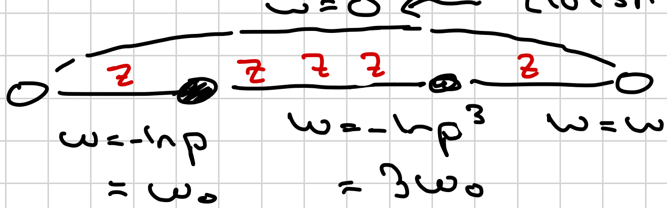


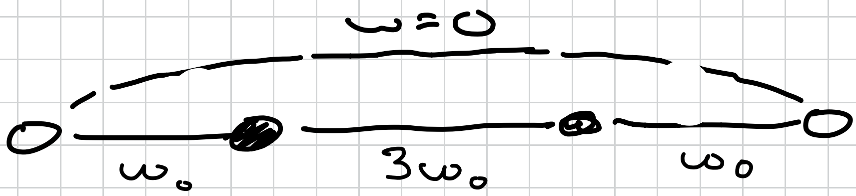
Add egdes reflecting the probability of an error triggering the two detectors

relative prob. of an error to no error $\longrightarrow$ weight $w = -\ln \frac{p_E}{1-p_E} \approx -\ln p_E > 0$ if $p_E \ll 1$

We have some prob p of a phase error

$w=0$ ← doesn't correspond to a real error, hence no weight



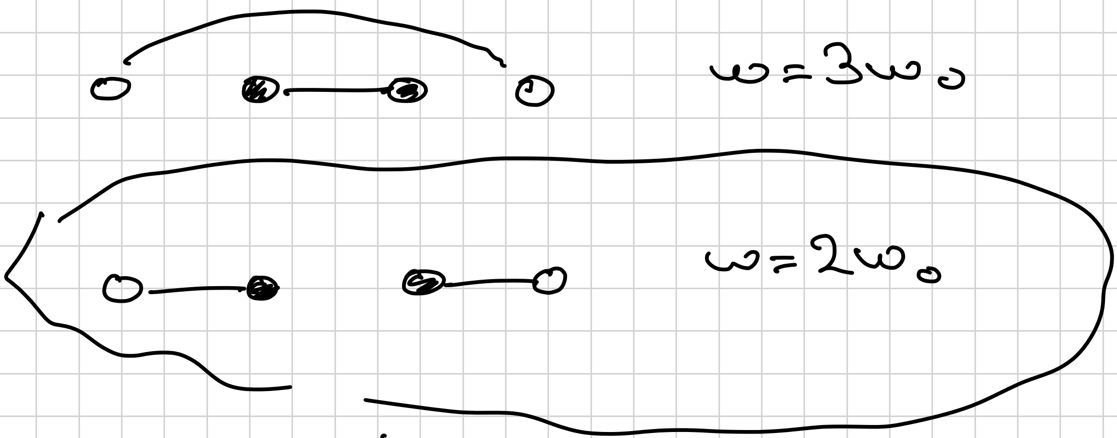


MWPM : Find <u>perfect</u> <u>matching</u> → all nodes should be paired

with <u>minimum</u> <u>weight</u> → edges that are used for matching should min. total weight

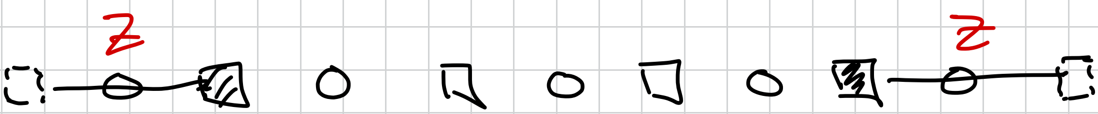
Blossom algorithm works in polynomial time $T \sim (\text{nodes}^2 \times \text{edges})$

Two possible matchings :



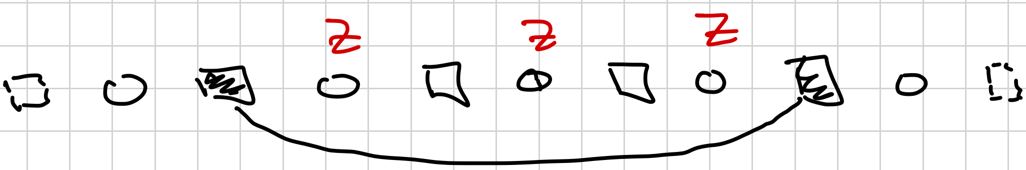
MWPM soulution

⇓ back to code



This is the most likely error!

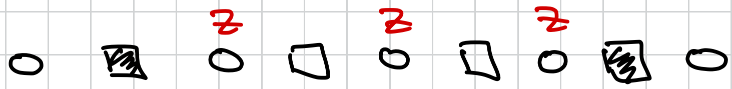
The other matching



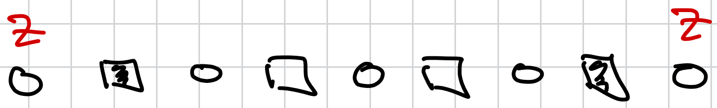
Possible error giving same syndrom, but less likely!

Equivalence classes of errors

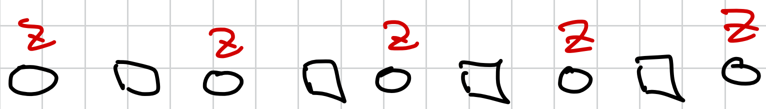
what if we have this error?



MWPM decoder $\Rightarrow$ correct with:



Error + Correction:



If we started with

$$|0\rangle_L = |+++++\rangle \overset{E+C}{\rightsquigarrow} |-----\rangle = |1\rangle_L$$

logical bitflip $X_L = ZZZZZ$

Unavoidable error $P_L \sim p^3$ logical error rate

in general

$$P_L \sim p^{\left(\frac{d+1}{2}\right)}$$

The two errors $E_1 = ZIIIZ$ and $E_2 = IZZZI$ are in different equivalence classes.

They correspond to the same syndrome, but are not equivalent as they are not connected by a stabilizer, but by a logical $E_2 = X_L E_1$

Let's define $Z_L = X_1$

$$Z_L = \begin{array}{ccccc} X & I & I & I & I \\ \circ & \circ & \circ & \circ & \circ \end{array}$$

(We can pick any qubit, they are equivalent up to stabilizer operations:

e.g. $S_1 X_1 = X_1 X_2 X_1 = X_2$)

- $Z_L |0\rangle_L = X_1 |+++++\rangle = + |0\rangle_L$

$Z_L |1\rangle_L = X_1 |-----\rangle = - |0\rangle_L$

$$Z_L (\alpha |0\rangle_L + \beta |1\rangle_L) = \alpha |0\rangle_L - \beta |1\rangle_L$$

logical phase flip

- $\{Z_L, X_L\} = \{X_1, Z_1 Z_2 Z_3 Z_4 Z_5\} =$

$\underbrace{\{X_1, Z_1\}}_{X_1 Z_1 + Z_1 X_1 = 0} Z_2 Z_3 Z_4 Z_5 = 0$

- Z_L and X_L are logical Pauli operators

- We can define equivalence classes as

class I if $[E, Z_L] = 0$ ← $E_2 = IZZZI$

class Z if $\{E, Z_L\} = 0$ ← $E_1 = ZIIIZ$

(The definition depends on our choice of Z_L, but not physically important. What matters is if errors are in same or different class.)

Other errors in same equivalence class:

Ex. $E_3 = S_1 E_2 = X_1 X_2 Z_2 Z_3 Z_4 = X_1 Y_2 Z_3 Z_4$ (up to irrel. phase)

in class I $\quad \sim p^4$

if X & Y errors also have prob p

$E_4 = S_1 E_1 = X_1 X_2 Z_1 Z_5 = Y_1 X_2 Z_5 \sim p^3$

in class Z

Optimal decoder

- Find most likely equivalence class of errors

In general a computionally hard problem

Number of errors consistent with a syndrom (in each class) $= 2^{\# \text{stabilizer}}$

Worse if there are measurement errors!

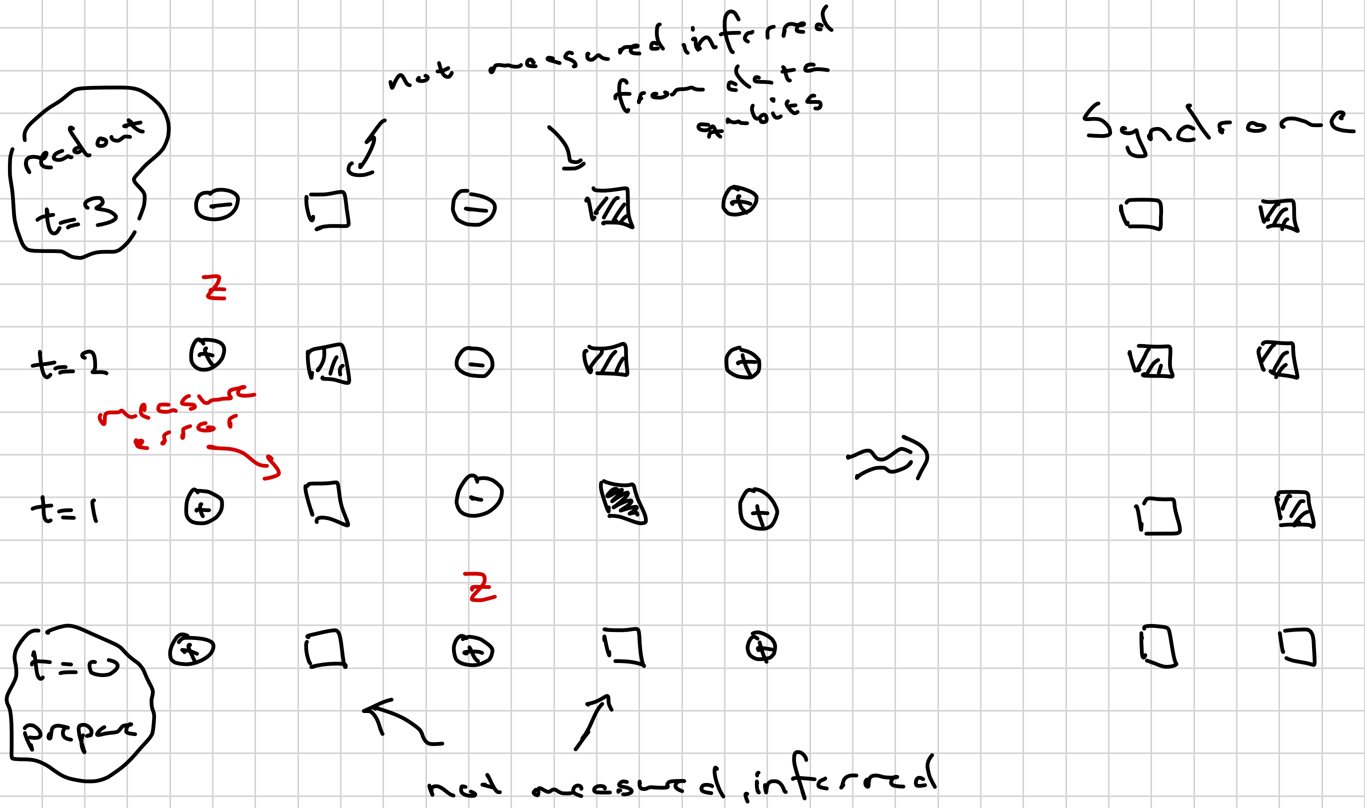
The Detector graph and decoding with measurement errors

○ = data qubit ⊕ = data qubit with phase error

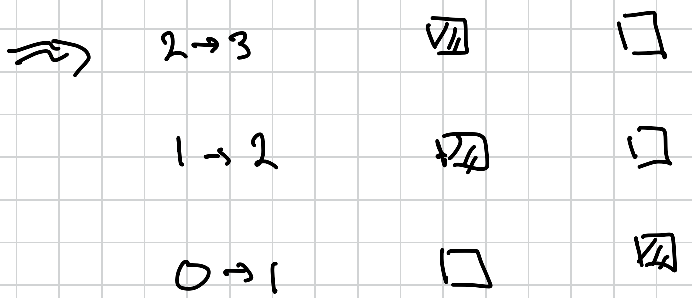
□ = ancilla 0

▨ = ancilla 1 (triggered ancilla)

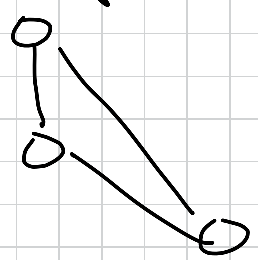
Memory experiment



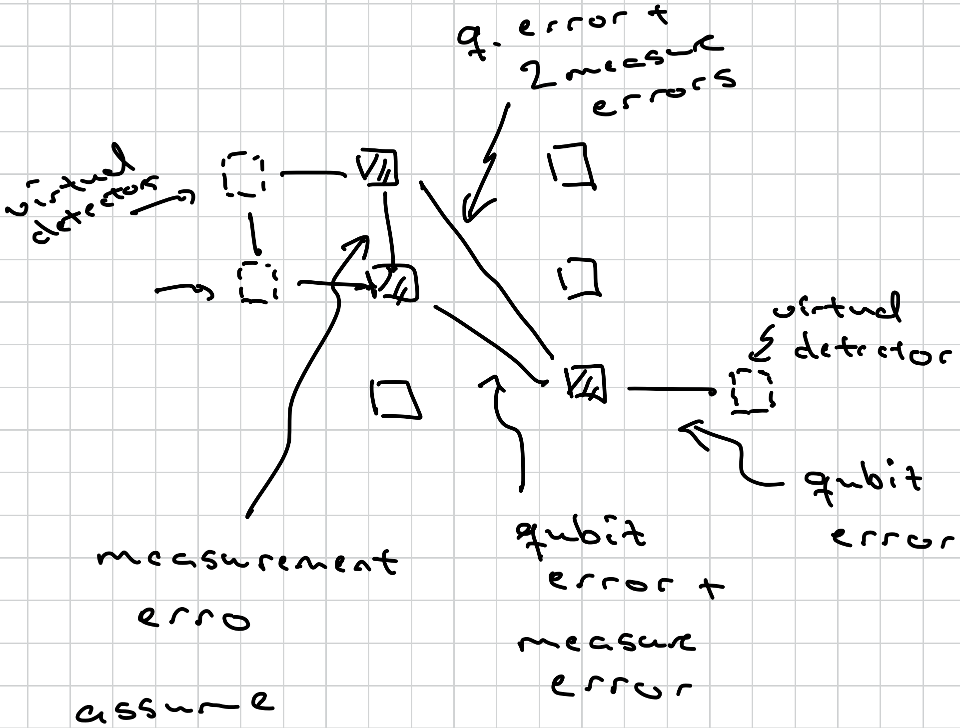
Detectors (changes)



Detector graph (or syndrome graph)



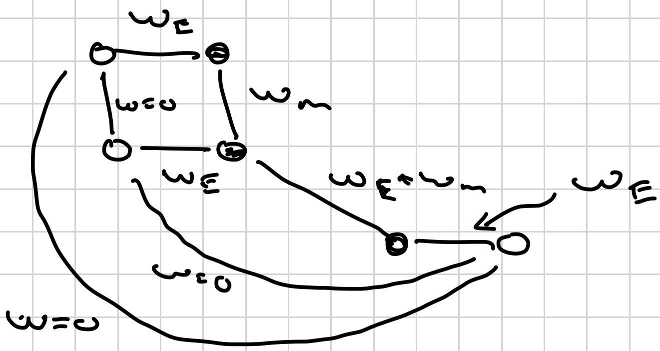
decoder ⟸ based on this we want to identify the errors



assume

phase error prob. p_E $\Rightarrow$ $w_E = -\ln \frac{p_E}{1-p_E}$

measure error prob. p_m $\Rightarrow$ $w_m = -\ln \frac{p_m}{1-p_m}$



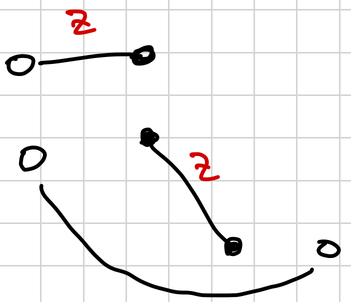
Decode with MWPM

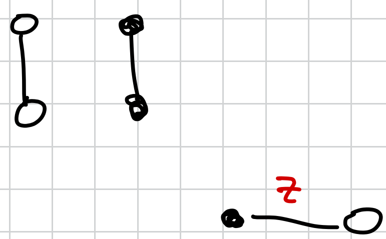
The point

Decoding is complicated, but crucial

Affects the logical error rate

Two low-weight matchings:





more likely correct with this

$w = 2w_E + w_m$ | $w = w_E + w_m$

$E_1 = ZZI$ $E_2 = IIZ$

in different equivalence class!

if actual error $E = ZZI$ then $E + C = X_L$!

The surface code

Repetition code can only correct bit or phase errors

e.g. $S_1 = X_1 X_2 \quad S_2 = X_2 X_3$

$|0\rangle_L = |{+}{+}{+}\rangle \quad |1\rangle_L = |{-}{-}{-}\rangle$

$X_1 (\alpha |0\rangle_L + \beta |1\rangle_L) = \alpha |0\rangle_L - \beta |1\rangle_L$

Single bit-flip error acts a logical phase-flip $Z_L = X_1$

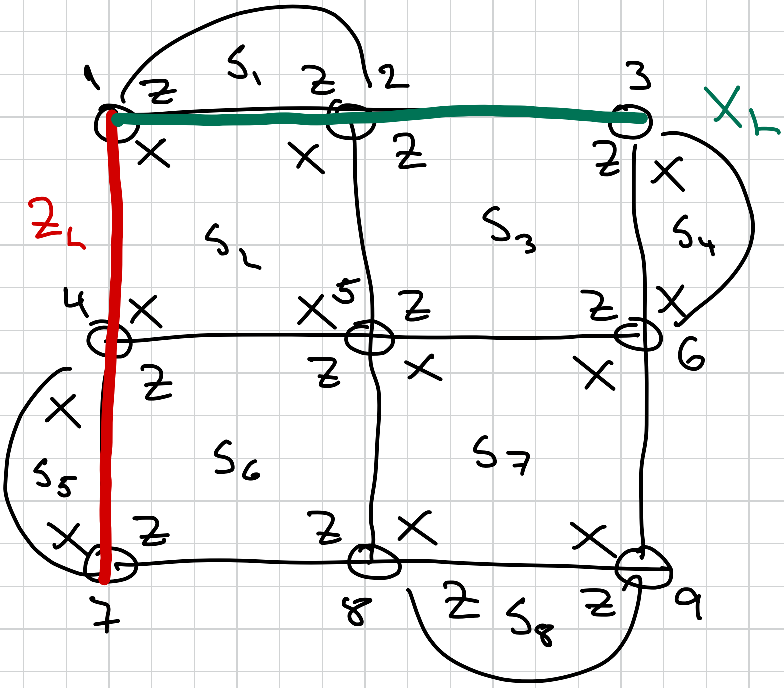
$\therefore$ it's not a functional QEC code (unless the noise is extremely biased, i.e. $p_X \ll p_Z$)

Consider instead the <u>surface</u> <u>code</u> (see also toric code)

- Two types of stabilizers all X to detect phase errors and all Z to detect bit errors.

- Defined on a $d \times d$ grid, with d^2 data qubits
  $d^2 - 1$ stabilizers (generators)
  $\updownarrow$
  $d^2 - 1$ ancilla/measure qubits

$d=3$ code



code-distance = minimal weight of a logical operator

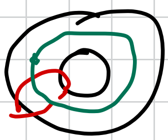
easily scaled up by adding more plaquettes

- stab. $S_1 = Z_1 Z_2$ $S_2 = X_1 X_2 X_4 X_5$, etc.

- logical operators $Z_L = Z_1 Z_4 Z_7$

$X_L = X_1 X_2 X_3$

On a torus these are incontractable loops



such codes are called topological codes

Z_L & X_L are the only two operators (up to products with stabilizers) that commute with all S, but are not part of the stabilizer group. (i.e. cannot be constructed from stabilizers)

∴ There is <u>one</u> logical qubit

$S_i|0\rangle_L = |0\rangle_L \quad S_i|1\rangle_L = |1\rangle_L \quad$ all $i = 1, \ldots, 8$

define $|0\rangle_L$: $Z_L|0\rangle_L = |0\rangle_L$

then $|1\rangle_L \equiv X_L|0\rangle_L$

$$\left(\begin{array}{l} \text{and consequently} \\ Z_L|1\rangle_L = Z_L X_L|0\rangle_L = -X_L Z_L|0\rangle_L = \\ \qquad = -X_L|0\rangle_L = -|1\rangle_L \end{array} \right)$$

Decoding the surface code

Example error