(II) Quantum error correction.

As we have seen along the lectures, quantum computing exploits two *total* properties of quantum mechanics :

- the superposition principle : quantum systems can be in coherent superpositions of "classical" states.

- the existence of entanglement (non-local correlations) among $\neq$ parts of a physical system.

  $\Rightarrow$ If one looks at only part of the system, one can only decipher very little info encoded in the system.

The properties are however extremely fragile and tend to decay very rapidly because the system is inevitably in contact with its environment.

The interaction btw system and environment makes them correlated, and eventually, the info that we encoded in the QC becomes encoded, instead, in the correlations btw the device and the envt.

At this point, we can no longer access the info by observing only the device $\Rightarrow$ the info is lost, and the QC crashes.

$\Rightarrow$ Decoherence causes errors that degrade quantum information.

In fact, decoherence is not the only issue. Even if we were able to perfectly isolate our device from its environment, we have seen previously that quantum gates (which in principle form a continuum of transformations) cannot be implemented with perfect accuracy. The implemented gate $\tilde{U}$ will differ from the desired transfo U by a small error ε.
If the computation requires many gates, these small imperfections will accumulate, and can, eventually, result in failure of the computation.

$\Rightarrow$ we need to protect the quantum computation against both decoherence and small unitary errors (faulty gates)

Errors due to noise can be treated with "quantum error correcting codes", while "fault tolerant quantum computing" also takes care of the fact that gates are imperfect.

1 Quantum Error Correcting Codes

→ how to protect quantum information from noise.

→ General idea: "encode" quantum states in a way that make resilient against the effect of noise, and then "decode" when one wishes to recover the original state.

* classical error correction:

In classical information, the simplest error-correcting codes are "repetition codes": we replace the bit we wish to protect by copies of it:

e.g.: $0 \rightarrow 000$

$1 \rightarrow 111$

Classically the error that may occur is a bit flip, say with proba p, for each bit.

If a bit flip occurs, say one the left bit we have

$$000 \to 100$$

$$111 \to 011$$

By "majority voting", we can still infer the original message (assuming that p is not too high).

For instance, if we received "100", we would say that it is likely that the left bit has flipped and thus the original message must be "0".

Majority voting would fail if more than one bit flips. → what is the proba ?

$$\begin{cases} \text{proba for zero bit to flip} = (1-p)^3 \\ \text{——— one ———} = (1-p)^2 p \times 3 \\ \text{——— two ———} = (1-p) p^2 \times 3 \\ \text{——— three ———} = p^3 \end{cases}$$

⇒ proba that 2 or 3 bits flip is

$$P_{err} = 3(1-p)p^2 + p^3 = 3p^2 - 2p^3$$

$P_{err} < p$ for $3p^2 - 2p^3 < p$

proba of error with error-correcting code.

proba of error without error-correcting code.

i.e. for $p < 1/2$.

Thus this repetition error-correcting code makes the transmission more reliable if $p < 1/2$.

This can be improved due to arbitrarely good reliability if we repeat the message N times ("N-bit repetition code") with N large enough.

* <u>Quantum Error Correction</u> :

Now we would like to apply similar ideas to develop codes that would protect quantum states against noise.

We can immediately think about potential difficulties, due to the differences btw classical and quantum information.

- <u>no cloning</u> : arbitrary quantum states cannot be copied (no-cloning thm).

- <u>errors are continuous</u> : classically, bit flip is the only error that can occur but quantum info is continous and thus, a continuum of errors may occur on a single qubit. Determining which error has occured in order to correct it at first appears to require infinite precision (and thus infinite resources).

- <u>measurement destroys information</u> :

In the classical procedure above, we observe the output from the channel to detect and correct the error.
In quantum mechanics, observing (measuring) the state generally destroys/disturbs it, and thus would make recovery impossible.

Fortunately, we will see that these problems can be overcome.

We will start by describing quantum-error correcting codes for the simplest cases (bit-flip and phase-flip channels) and then discuss a general procedure.

1_ The bit-flip channel

Let's start with the simple example: the quantum analogous of the classical bit-flip channel described above.

Remember from previous lecture: the bit-flip channel leaves an input qubit state intact with proba $(1-p)$, and applies $\hat{X}$ with proba p:

$$\rho \mapsto \mathcal{E}(\rho) = (1-p)\,\rho + p\, X\rho X$$

Suppose we start from a (pure) state $|\psi\rangle$ with

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

We encode this single-qubit state with 3 qubits:

$$\begin{cases} |0\rangle \longrightarrow |0_L\rangle \equiv |000\rangle \\ |1\rangle \longrightarrow |1_L\rangle \equiv |111\rangle \end{cases}$$

that is :

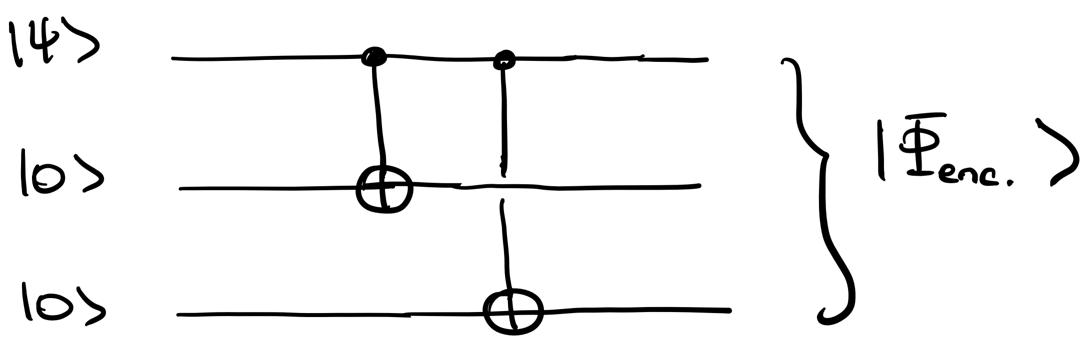
$$|\psi\rangle \longrightarrow a|0_L\rangle + b|1_L\rangle$$
$$= a|000\rangle + b|111\rangle$$
$$= |\Phi_{enc.}\rangle$$

Note :

The index L stands for "logical", as opposed to "physical".

Physical qubits are the actual qubits in the quantum computer, while logical qubits are groups of physical qubits used as if they were single qubits.

Circuit for encoding :



$$|00\psi\rangle = a|000\rangle + b|001\rangle$$
$$\xrightarrow{CNOT} a|000\rangle + b|011\rangle$$
$$\xrightarrow{CNOT} a|000\rangle + b|111\rangle = |\Phi_{enc.}\rangle$$

Suppose encoding has been done perfectly. Now each of the 3 qubits goes through the bit-flip channel (independently) and has a proba p of being flipped.

$\Rightarrow$ Possible cases and effect on the encoded state $|\Phi_{enc}\rangle$:

case	proba	output state
0 flip	$(1-p)^3$	(0) $\leftarrow$ $\vert\Phi_{enc}\rangle$
1 flip	$3p(1-p)^2$	$\vert\tilde{\Phi}^{(1)}_{enc}\rangle$ (1) $\leftarrow$ $= a\vert 100\rangle + b\vert 011\rangle$ or (2) $\leftarrow$ $= a\vert 010\rangle + b\vert 101\rangle$ or (3) $\leftarrow$ $= a\vert 001\rangle + b\vert 110\rangle$
2 flips	$3p^2(1-p)$	$\vert\tilde{\Phi}^{(2)}\rangle$ $= a\vert 110\rangle + b\vert 001\rangle$ or $= a\vert 011\rangle + b\vert 100\rangle$ or $= a\vert 101\rangle + b\vert 010\rangle$
3 flips	p^3	$\vert\tilde{\Phi}^{(3)}\rangle$ $= a\vert 111\rangle + b\vert 000\rangle$

If a bit-flip has occured on at most one qubit, there is (like in the classical case) a simple quantum-error correction procedure that can be used to recover the correct state $|\psi\rangle$.

This procedure goes in two steps:

1) Error detection or syndrome diagnosis:

We perform a measurement that tells us, what error (if any) has occured on $|\Phi_{enc}\rangle$, i.e. we want to be able to tell if the 3-qubit state after the channel is (0), (1), (2) or (3)

but ⚠ this measurement should not reveal the state (a, b) otherwise would destroy it.

=> we measure the proba of being in the subspaces spanned by:

$$\{|000\rangle, |111\rangle\} \rightarrow (0)$$
$$\{|100\rangle, |011\rangle\} \rightarrow (1)$$
$$\{|010\rangle, |101\rangle\} \rightarrow (2)$$
$$\{|001\rangle, |110\rangle\} \rightarrow (3)$$

The corresponding projectors are :

$$\hat{P}_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

$$\hat{P}_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$\hat{P}_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$\hat{P}_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

For example if the left qubit has flipped i.e. if after the channel the 3-qubit state is

$$|\tilde{\Phi}^{(1)}\rangle = a|100\rangle + b|011\rangle$$

then the result of the measurements are

$$\langle\tilde{\Phi}^{(1)}|\hat{P}_0|\tilde{\Phi}^{(1)}\rangle = 0$$ = proba of being in subspace (0)

$$\langle\tilde{\Phi}^{(1)}|\hat{P}_1|\tilde{\Phi}^{(1)}\rangle = |a|^2 + |b|^2 = 1$$ (normalizat°)

$$\langle\tilde{\Phi}^{(1)}|\hat{P}_2|\tilde{\Phi}^{(1)}\rangle = \langle\tilde{\Phi}^{(1)}|\hat{P}_3|\tilde{\Phi}^{(1)}\rangle = 0$$

the projectors corresp. to mutually exclusive outcomes (only one will be 1, others will be 0)

$\Rightarrow$ we know for sure that the first qubit has flipped (supposing that at most one qubit has flipped).

Note: The measurem^t result is called "error syndrom".

What is important is that the error syndrom only tells us which bit has flipped, and does not tell anything about a or b, i.e it does not contain info about the state $|\psi\rangle$ that we want to protect.

Thus, the state is not perturbed.

Indeed, the post-measurement state is:

$$\frac{\hat{P}_1 |\tilde{\Phi}^{(1)}\rangle}{\| \hat{P}_1 |\tilde{\Phi}^{(1)}\rangle \|} = a|100\rangle + b|011\rangle = |\tilde{\Phi}^{(1)}\rangle$$

Note: there is a different way of doing the error detection that is useful to generalize to the case of more than 3 qubits:

Instead of measuring the four projectors P_0, P_1, P_2, P_3, we can perform two measurements corresponding to the observables:

$$\rightarrow \quad Z \otimes Z \otimes \mathbb{1}$$
$$\rightarrow \quad \mathbb{1} \otimes Z \otimes Z$$

Both of them have eigenvalues ± 1, thus each of the 2 measurements give one bit of info $\Rightarrow$ 2 bits in total, i.e. 4 possibilities.

The first measurement allows to compare the left and middle qubits, i.e. will give $+1$ if they are both $|0\rangle$ or $|1\rangle$, and will give -1 if one is in $|0\rangle$ and the other $|1\rangle$.

e.g. $$\langle 000 | Z \otimes Z \otimes \mathbb{1} \, | 000 \rangle = +1$$

$$\langle 100 | Z \otimes Z \otimes \mathbb{1} \, | 100 \rangle = -1$$

since $\begin{cases} Z|0\rangle = |0\rangle \\ Z|1\rangle = -|1\rangle \end{cases}$

Similarly the second measurement ($I \otimes Z \otimes Z$) will compare the middle and right qubit.

Combining these will tell us whether a bit flip occured, and if so, on which qubit:

- if both measurements give $+1$ $\Rightarrow$ all 3 qubits are in the same state $\Rightarrow$ with high proba, no bit flip occured.
  (the other possibility would be that all 3 qubits have flipped but if p is small, this has smaller proba).

- if the 1st measurement gives $+1$, and the 2nd -1 $\Rightarrow$ left & middle qubits are the same, but middle & right ones are $\neq$ $\Rightarrow$ with high proba, the right one has flipped.
  (again could have flipped left & middle but smaller proba)

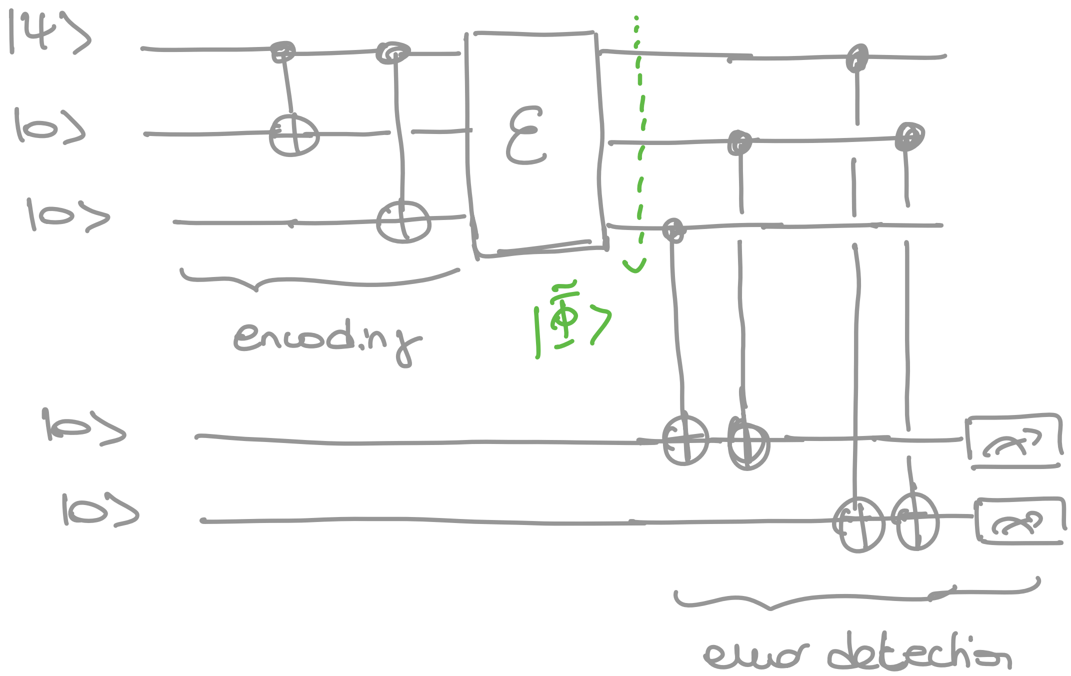
- if 1st meas gives -1, and 2nd gives $+1$ $\Rightarrow$ with high proba, the left qubit flipped.

- if both give -1 $\Rightarrow$ with high proba the middle has flipped

This way of doing error detection requires less measurements and can be more easily generalized to encoding on more than 3 qubits.

Again these measurements do not reveal the state and thus, do not disturb it.

In practice this can be realized by introducing 2 ancilla qubits (one for each op)



imagine left qubit has flipped:

$$|\tilde{\Phi}\rangle = a\,|\underline{\underline{1}}00\rangle + b\,|011\rangle$$

$$|00\rangle \otimes |\tilde{\Phi}\rangle \xrightarrow{\text{CNOT}} a\,|01\rangle \otimes |\underline{\underline{1}}00\rangle + b\,|01\rangle\,|\underline{\underline{0}}11\rangle$$

$$\xrightarrow{CNOT} a\, |01\rangle \otimes |1\underline{\underline{00}}\rangle + b\, |01\rangle |0\underline{\underline{11}}\rangle$$

$$= |01\rangle \otimes \big(\underbrace{a\, |100\rangle + b\, |011\rangle}_{|\tilde{\Phi}\rangle}\big)$$

actually not entangled

measure always give $|01\rangle$ & state $|\tilde{\Phi}\rangle$ not destroyed.

2) Recovery

Now that we know what error has occured, we can correct it to recover the original state.

For instance, if the left qubit has flipped we simply need to flip again (with an X gate)

$$|\tilde{\Phi}^{(1)}\rangle = a|100\rangle + b|011\rangle$$

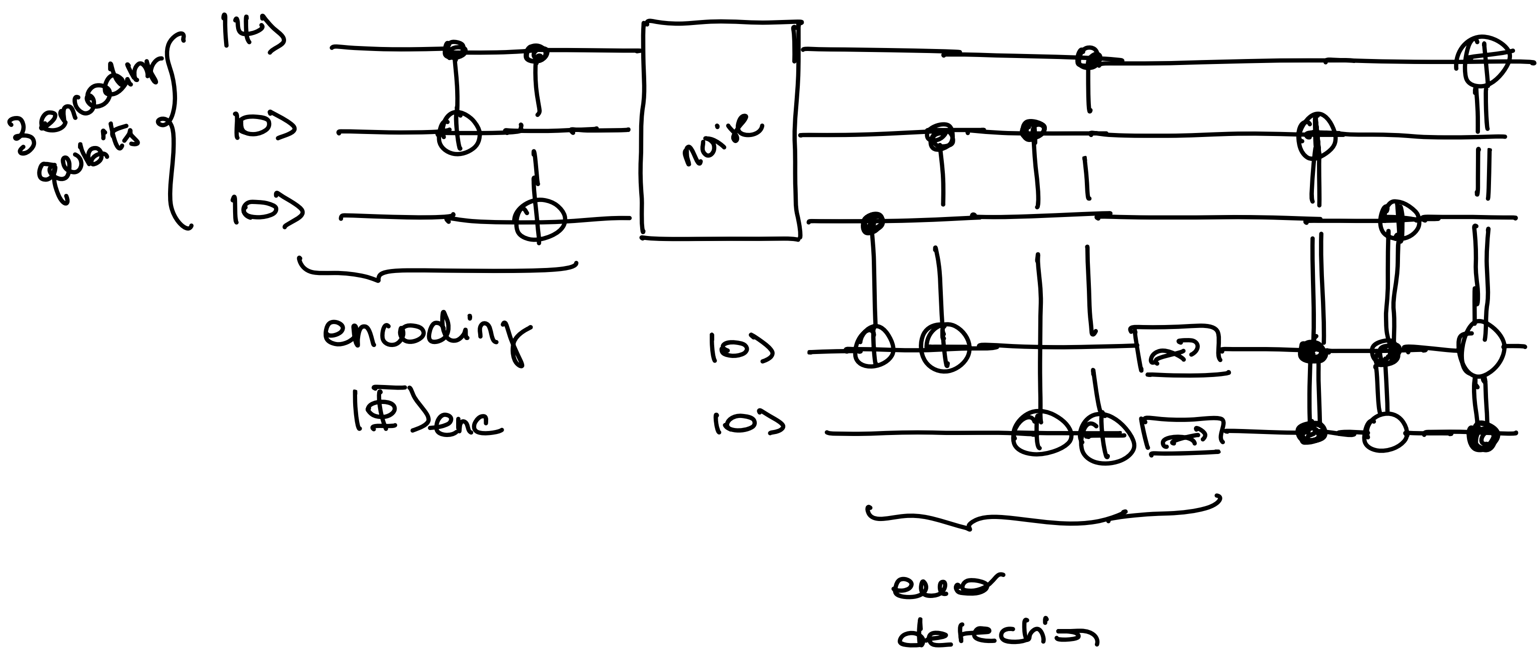
$$\xrightarrow{X \otimes 1 \otimes 1} a|000\rangle + b|111\rangle$$

Similarly, if instead the middle (or right) qubit has flipped we apply X on the middle (or right) qubit with

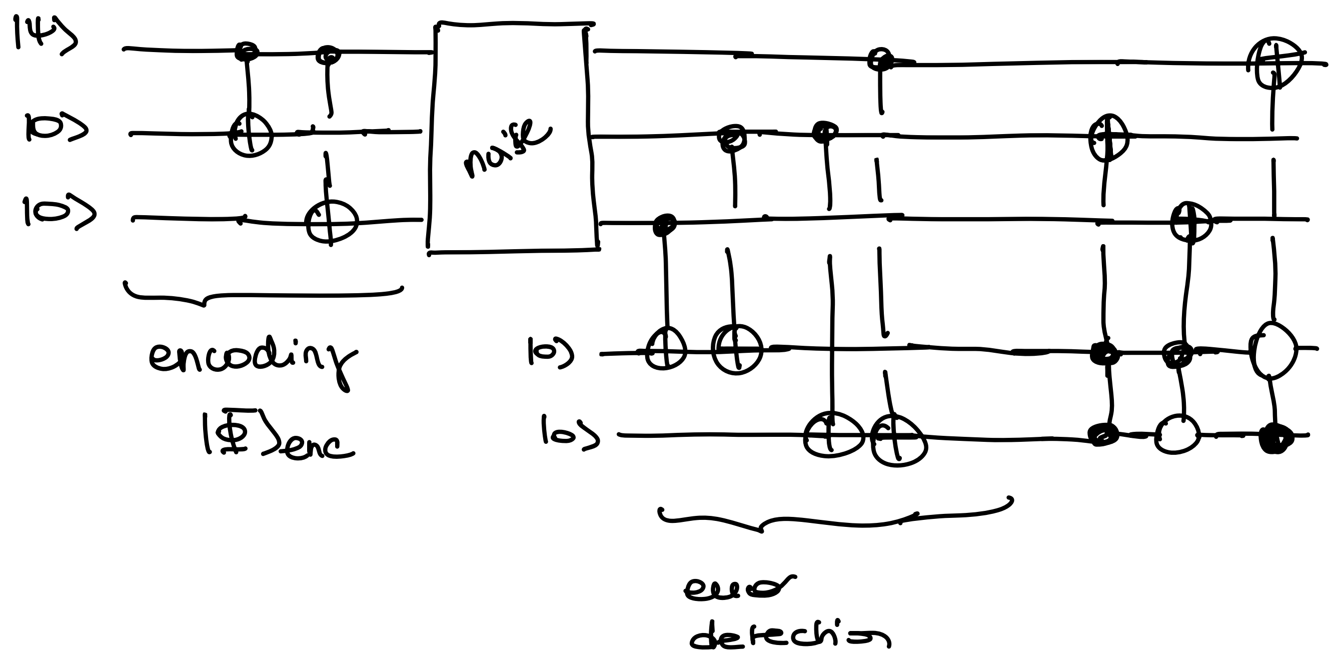
$$1 \otimes X \otimes 1 \quad (\text{or } 1 \otimes 1 \otimes X)$$

And of course, if we found from the error diagnosis that no qubit has flipped → do nothing.

The circuit can be represented as:



In fact measurements are not needed :



will correct for any bit flip. But measurements allow one to know which bit has flipped and to correct for that specific error (saves gate resources).

This error-correction procedure works perfectly provided that a bit flip has occured on at most one of the three qubits.

This occurs with probability:

$$(1-p)^3 + 3p(1-p)^2 = 1 - 3p^2 + 2p^3$$

The procedure will fail if two or three qubits undergo a bit flip. This occurs with probability

$$p_{err}^{QEC} = 3p^2 - 2p^3$$

(as in the classical case)

→ How does this compare to the case when no error correction is applied?

Like in the classical case we can see that if $p < 1/2$ then the proba of error with quantum error correction (QEC) p_{err}^{QEC} is smaller than the proba of error p without QEC:

$$p_{err}^{QEC} = 3p^2 - 2p^3 < p \quad \text{if } p < 1/2$$

But this does not provide a good error analysis in the quantum case -

Because of superposition, some errors have little or no effect on some states or very large effects on others.
For ex: a bit flip would have no effect on the state $|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$ while it has a large effect on the state $|0\rangle$.

In general because quantum states live in a continuous space $\Rightarrow$ some errors can corrupt the state by a very small amount, and others by large amounts.

$\Rightarrow$ To have a more meaningful error analysis, we make use of the fidelity btw quantum states ~ measure of the "distance" btw two states.

Aside:

→ Fidelity:

The distinguishability btw two pure states $|\psi\rangle$ and $|\phi\rangle$ can be quantified by their overlap $|\langle\psi|\phi\rangle|$, or rather by the deviation of this overlap from 1.

$|\langle\psi|\phi\rangle|$ is also called "fidelity".

More generally, the fidelity btw two density operators ρ and ρ' is defined by:

$$\boxed{F(\rho,\rho') = tr\left(\sqrt{\rho^{1/2}\,\rho'\,\rho^{1/2}}\right)}$$

- if $\rho' = |\psi\rangle\langle\psi|$ is a pure state

$$\boxed{\begin{aligned} F(\rho,\rho') &= tr\sqrt{\rho^{1/2}\,|\psi\rangle\langle\psi|\,\rho^{1/2}} \\ &= \sqrt{\langle\psi|\rho|\psi\rangle} \end{aligned}}$$

- <u>without QEC</u>:

initial 1-qubit state $|\psi\rangle = a|0\rangle + b|1\rangle$

$$\rho = |\psi\rangle\langle\psi| \longmapsto \mathcal{E}(\rho) = (1-p)\rho + p X\rho X$$

$\Rightarrow$ The fidelity btw $\rho = |\psi\rangle\langle\psi|$ and $\mathcal{E}(\rho)$ is:

$$F\Big(|\psi\rangle\langle\psi|, \mathcal{E}(\rho)\Big) = \sqrt{\langle\psi|\,\mathcal{E}(\rho)\,|\psi\rangle}$$

$$= \sqrt{\langle\psi|\Big[(1-p)|\psi\rangle\langle\psi| + p\,X|\psi\rangle\langle\psi|X\Big]|\psi\rangle}$$

$$= \sqrt{(1-p)\underbrace{\langle\psi|\psi\rangle^2}_{1} + p\underbrace{\langle\psi|X|\psi\rangle^2}_{\geq 0}}$$

which is minimum when $\langle\psi|X|\psi\rangle = 0$ (for instance when $|\psi\rangle = |0\rangle$ or $|1\rangle$).

$\Rightarrow$ The minimum fidelity is:

$$F(\mathcal{E}) = \sqrt{1-p} \quad \equiv F_{noQEC}$$

- with QEC : want to estimate

the fidelity btw the initial encoded 3-qubit state $|\Phi_{enc}\rangle = a|000\rangle + b|111\rangle$ and the output state after the noisy channel & the QEC.

This state is

$$\rho^{QEC} = \underbrace{\left[(1-p)^3 + 3p(1-p)^2 \right]}_{} |\Phi_{enc}\rangle\langle\Phi_{enc}|$$

↳ proba that the error was corrected and thus $|\Phi\rangle$ was recovered.

$$+ \underbrace{\cdots}_{}$$

↳ others terms representing contributions from 2 or 3 bit flips. (QEC has failed)

These are ≥ 0

$\Rightarrow$ the fidelity

$$F(|\Phi_{enc}\rangle\langle\Phi_{enc}|, \rho^{QEC}) \geq F(|\Phi_{enc}\rangle\langle\Phi_{enc}|, \bar{\rho}^{QEC})$$

where $\bar{\rho}^{QEC} = [(1-p)^3 + 3p(1-p)^2] |\Phi_{enc}\rangle\langle\Phi_{enc}|$
+ terms orthogonal to $|\Phi_{enc}\rangle\langle\Phi_{enc}|$

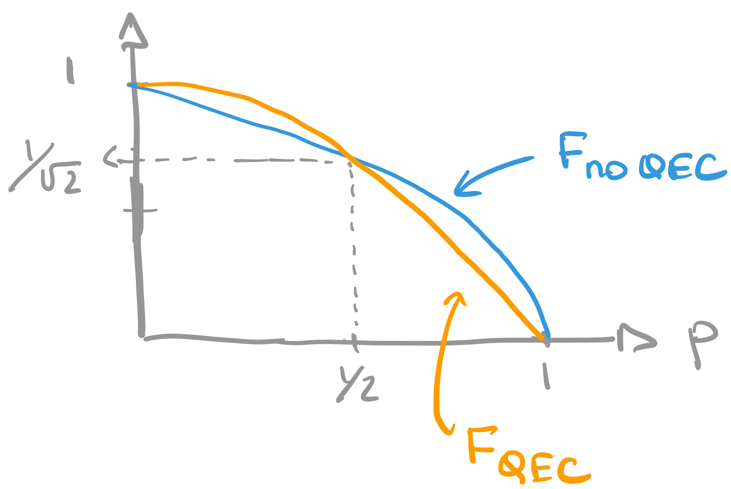
$\Rightarrow$

$$F\left(|\Phi_{enc}\rangle\langle\Phi_{enc}|, \bar{\rho}^{QEC}\right) = \sqrt{\langle\Phi_{enc}|\bar{\rho}^{QEC}|\Phi_{enc}\rangle}$$

$$= \sqrt{\left[(1-p)^3 + 3p(1-p)^2\right]}$$

$$= \sqrt{1-3p^2+2p^3}$$

$$\equiv F_{QEC}$$



For $p < 1/2 \Rightarrow$ the fidelity btw initial and corrupt (noisy) state is improved with QEC.

$p = 1/2$ is the "breaking point": for $p > 1/2$ the QEC makes things worse.

2- The phase-flip channel

The bit-flip was useful to understand the principle of QEC code, but as mentioned above, many other types of errors can occur to qubits.

A more interesting example is the phase-flip channel, which has no classical equivalent.

This channel maps:

$$\mathcal{E}_{\substack{\text{phase}\\ \text{flip}}} : \rho \longmapsto (1-p)\rho + p\, Z \rho Z$$

It turns out that we can treat this noise channel exactly in the same way as the bit flip, by working in the $\{|+\rangle, |-\rangle\}$ basis instead of the $\{|0\rangle, |1\rangle\}$ basis.

This is because $\begin{cases} Z\,|+\rangle = |-\rangle \\ Z\,|-\rangle = |+\rangle \end{cases}$

thus the Z operator acts like a bit flip in this basis.

This suggests to use $|{+}{+}{+}\rangle$ and $|{-}{-}{-}\rangle$ as the "logical 0 and 1" to protect the state against phase-flip errors.

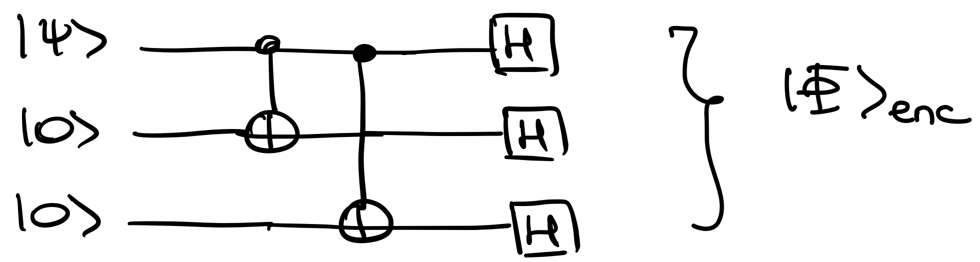
Everything is then the same wrt the $\{|+\rangle, |-\rangle\}$ basis instead of the $\{|0\rangle, |1\rangle\}$ basis.

Thus the procedure is :

0) <u>Encoding</u> :

$$\begin{cases} |0_L\rangle \equiv |{+}{+}{+}\rangle \\ |1_L\rangle \equiv |{-}{-}{-}\rangle \end{cases}$$

circuit :



0') State goes through <u>noisy channel</u> $\mathcal{E}^{\otimes 3}$:

effect of a phase error on e.g. the left qubit :

$$a|{+}{+}{+}\rangle + b|{-}{-}{-}\rangle \mapsto a|{-}{+}{+}\rangle + b|{+}{-}{-}\rangle$$

1) Error detection :

- As before we can do 4 measurements projecting into subspaces

$$\{ |+++\rangle\langle +++| + |---\rangle\langle ---| \}$$

$$\{ |-++\rangle\langle -++| + |+--\rangle\langle +--| \}$$

etc...

The projectors are the same but conjugated with Hadamard gates :

$$H^{\otimes 3} P_j H^{\otimes 3}$$

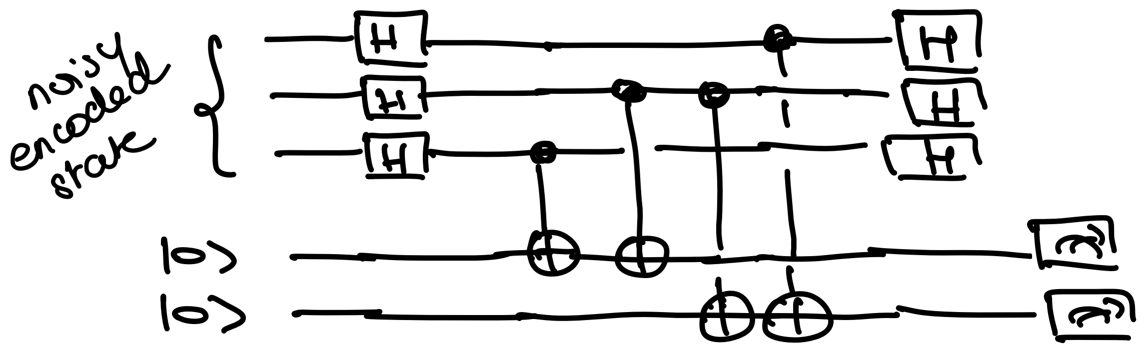
- Alternatively we can do 2 measurements of

$$\begin{cases} X \otimes X \otimes \mathbb{1} \\ \mathbb{1} \otimes X \otimes X \end{cases}$$

which compare the signs of two qubit states.

$$\text{Since } \begin{cases} XX\mathbb{1} = H^{\otimes 3} \; ZZ\mathbb{1} \; H^{\otimes 3} \\ \mathbb{1}XX = H^{\otimes 3} \; \mathbb{1}ZZ \; H^{\otimes 3} \end{cases}$$

$\Rightarrow$ this can be achieved with :



See that this works: for ex

if the left qubit had a phase flip:

state after noise:

$$|00\rangle \left(a\,|{-}{+}{+}\rangle + b\,|{+}{-}{-}\rangle \right)$$

$$\xmapsto{H^{\otimes 3}} |00\rangle \left(a\,|100\rangle + b\,|011\rangle \right)$$

$$\xmapsto{\text{CNOTs}} |01\rangle \left(a\,|100\rangle + b\,|011\rangle \right)$$

$$\xmapsto{\text{CNOTs}} |01\rangle \left(a\,|100\rangle + b\,|011\rangle \right)$$

$$\xmapsto{H^{\otimes 3}} |01\rangle \left(a\,|{-}{+}{+}\rangle + b\,|{+}{-}{-}\rangle \right)$$

measure ancillas :

$\Longrightarrow$ know that left qubit has flipped

& have not destroyed the encoded state

2) Recovery

consists of the same operations as for the bit flip channel, but conjugated with Hadamard $\Rightarrow$ instead of applying X to the flipped qubit, we apply $HXH = Z$ to correct the phase.

The error analysis is the same as for the bit-flip code, in particular the minimum fidelity is the same.

These 2 channels are said to be "unitarily equivalent".