LECTURE 2
INTRODUCTION TO QUANTUM ERROR CORRECTING CODES

Advanced Quantum Information and Computing

Thomas Debris-Alazard

Inria, École Polytechnique

- Suppose that you store bits on your device and your memory is altered:

$$001011 \rightsquigarrow 001111$$

- Suppose that you perform your computations with non-perfect elementary gates, for instance:

$$1 \xrightarrow{\texttt{NOT}} 0 \text{ but sometimes } 1 \xrightarrow{\texttt{NOT}} 1$$

How can we protect bits against the noise?

Do what you do in your everyday life:

Add redundancy!

An example: spell your name over the phone, send first names!

M like Mike, O like Oscar, R like Romeo, A like Alpha, I like India and N like November

- We perform an encoding $\big($*i.e.*, adding redundancy$\big)$,

  $$\text{M} \mapsto \text{Mike},\ \text{O} \mapsto \text{Oscar},\ \text{R} \mapsto \text{Romeo},\ \text{A} \mapsto \text{Alpha, etc.}\ldots$$

- If the information is altered $\big($for instance when having a bad communication over the phone$\big)$,

  $$\text{Mike} \xrightarrow{\textit{noise}} \text{“ike”},\ \text{Oscar} \xrightarrow{\textit{noise}} \text{“scar”},\ \text{Romeo} \xrightarrow{\textit{noise}} \text{“meo”},\ \text{Alpha} \xrightarrow{\textit{noise}} \text{“ alph”}$$

- The receiver can perform a decoding: recovering the first names and then the letters,

  $$\text{“ike”} \to \text{Mike} \to \text{M},\ \text{“sca”} \to \text{Oscar} \to \text{O},\ \text{“meo”} \to \text{Romeo} \to \text{R},\ \text{“alph”} \to \text{Alpha} \to \text{A}$$

The first example of error-correcting codes:

3-repetition code:

- **Encoding**: $b \in \{0,1\} \longmapsto bbb \in \{0,1\}^3$
- **Noisy Channel**: $bbb \longmapsto c_1c_2c_3$
- **Decoding Strategy**: given $c_1c_2c_3 \in \{0,1\}^3$, choose the majority bit

$$001 \longmapsto 0,\ 011 \longmapsto 1,\ 101 \longmapsto 1, \text{etc.}\ldots$$

$\longrightarrow$ This decoding strategy is successful if there are < 2 bits which are changed!

Exercise:

Why haven't we introduced the 2-repetition code?

Without efficient error correcting codes

- Storing reliably data would be impossible
- Computations on our computers would be most of the time false
- We couldn't send and download information on Internet

False intuition: we only need to improve our devices

No! Think that devices are subject to external constraints. Furthermore, in the case of telecommunications, do you hope to be able to receive all the bits from a photo taken by a satellite around Mars? Would you be happy with only half of the bits of the photo?

$\longrightarrow$ Error correcting codes were the cornerstone of the development of computers and telecommunications!

Building an efficient quantum computer?

Let's go $\Big($good luck. . . $\Big)$! But it is impossible to build architectures that are **completely isolated from the environment: decoherence** $\Big($pure states $\mapsto$ mixed states$\Big)$

Decoherence ($\longleftrightarrow$ Quantum Noise):

There will be "noise" during computations that will modify the results. . .

- What does the "**noise**" mean in the quantum case?
- How to be "**protected**" against the "noise"? Can we also add redundancy as in the classical case?

Protect against errors in the quantum world: a much harder problem!

- **Problem** 1: Not enough to protect $|0\rangle$ and $|1\rangle$, every linear combinations $\alpha |0\rangle + \beta |1\rangle$ must be protected as well
- **Problem** 2: Much richer error model than for classical bits $\big($not only "flip"...$\big)$
- **Problem** 3: Impossibility to copy qubits before working on it $\big($no cloning theorem$\big)$
- **Problem** 4: Measurements modify the qubits...

To overcome these issues: we will be inspired by the classical case!

Presentation of quantum error correcting codes!

Quantum error correcting code are (roughly):

- a clever use of classical codes and (syndrome) projective measurements

1. A First Quantum Error Correcting Code: Shor's Code
2. Calderbank-Shor-Steane $\left(\text{CSS}\right)$ Codes
3. Stabilizer Codes
4. Threshold Theorem

SHOR'S QUANTUM CODE

Inspired by the classical case: repetition code?

$$\alpha |0\rangle + \beta |1\rangle \longmapsto (\alpha |0\rangle + \beta |1\rangle)^{\otimes 3}$$

But is it possible?

Inspired by the classical case: repetition code?

$$\alpha |0\rangle + \beta |1\rangle \longmapsto (\alpha |0\rangle + \beta |1\rangle)^{\otimes 3}$$

But is it possible?

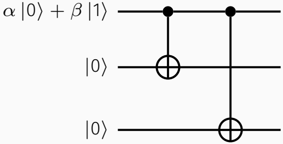
No! No-cloning theorem. . .

Instead consider the following encoding to "mimic the repetition code":

$$(\alpha |0\rangle + \beta |1\rangle) \otimes |00\rangle \longmapsto \alpha |000\rangle + \beta |111\rangle$$

$\longrightarrow$ It is not a repetition code!

To perform encoding, following quantum circuit:



Errors of type X (flipping)

Inspired by the classical case: flip the qubits, i.e. apply X

Error X on the second qubit:

$$\alpha |000\rangle + \beta |111\rangle \rightsquigarrow \alpha |010\rangle + \beta |101\rangle$$

But how to correct this error?

Inspired by the classical case: flip the qubits, i.e. apply X

Error X on the second qubit:

$$\alpha |000\rangle + \beta |111\rangle \rightsquigarrow \alpha |010\rangle + \beta |101\rangle$$

But how to correct this error?

Use a parity-check matrix!

$H \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ parity-check matrix of the 3-repetition code $\{(000), (111)\}$

$\longrightarrow$ applying to either (010) or (101) gives $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ showing an error occurred to the second bit

Quantumly: implement $|x\rangle \otimes |00\rangle \mapsto |x\rangle \otimes |xH^{T}\rangle$ and apply it to

$$(\alpha |010\rangle + \beta |101\rangle) \otimes |00\rangle \longmapsto (\alpha |010\rangle + \beta |101\rangle) \otimes |11\rangle$$

Measure the last two registers and deduce where the X error occurred

$\longrightarrow$ apply X on the qubit where there is an error leading to the original quantum state $\left(X^2 = I_2\right)$

This method enables to correct any X on one qubit

But is it necessary to introduce two ancillary qubits?

Using two auxiliary qubits and **H** was an artefact to mimic the classical case!

$$\alpha |000\rangle + \beta |111\rangle \rightsquigarrow \text{ error?}$$

(*i*) No error,

$$\alpha |000\rangle + \beta |111\rangle \in \mathcal{C}_0 \stackrel{\text{def}}{=} \text{Vect}\left(|000\rangle, |111\rangle\right)$$

If an error **X** occurs we will be in one of the following situations:

(*ii*) First qubit,

$$\alpha |100\rangle + \beta |011\rangle \in \mathcal{C}_1 \stackrel{\text{def}}{=} \text{Vect}\left(|100\rangle, |011\rangle\right)$$

(*iii*) Second qubit,

$$\alpha |010\rangle + \beta |101\rangle \in \mathcal{C}_2 \stackrel{\text{def}}{=} \text{Vect}\left(|010\rangle, |101\rangle\right)$$

(*iv*) Third qubit,

$$\alpha |001\rangle + \beta |110\rangle \in \mathcal{C}_3 \stackrel{\text{def}}{=} \text{Vect}\left(|001\rangle, |110\rangle\right)$$

The $\mathcal{C}_x$'s are the cosets and are orthogonal!

$\longrightarrow$ It defines a measurement: we can decide in which space we live and removing the error

(I) Fundamental idea: decompose the three qubits space as (coset decomposition)

$$\left(\mathbb{C}^2\right)^{\otimes 3} = \mathcal{C}_0 \overset{\perp}{\oplus} \mathcal{C}_1 \overset{\perp}{\oplus} \mathcal{C}_2 \overset{\perp}{\oplus} \mathcal{C}_3 \tag{1}$$

where,

$$\mathcal{C}_0 \overset{\text{def}}{=} \text{Vect}\left(|000\rangle, |111\rangle\right), \quad \mathcal{C}_1 \overset{\text{def}}{=} \text{Vect}\left(|100\rangle, |011\rangle\right), \quad \mathcal{C}_2 \overset{\text{def}}{=} \text{Vect}\left(|010\rangle, |101\rangle\right)$$

$$\mathcal{C}_3 \overset{\text{def}}{=} \text{Vect}\left(|001\rangle, |110\rangle\right)$$

(I) Fundamental idea: decompose the three qubits space as (coset decomposition)

$$\left(\mathbb{C}^2\right)^{\otimes 3} = \mathcal{C}_0 \overset{\perp}{\oplus} \mathcal{C}_1 \overset{\perp}{\oplus} \mathcal{C}_2 \overset{\perp}{\oplus} \mathcal{C}_3 \tag{1}$$

where,

$$\mathcal{C}_0 \overset{\text{def}}{=} \text{Vect}\left(|000\rangle\,, |111\rangle\right), \quad \mathcal{C}_1 \overset{\text{def}}{=} \text{Vect}\left(|100\rangle\,, |011\rangle\right), \quad \mathcal{C}_2 \overset{\text{def}}{=} \text{Vect}\left(|010\rangle\,, |101\rangle\right)$$

$$\mathcal{C}_3 \overset{\text{def}}{=} \text{Vect}\left(|001\rangle\,, |110\rangle\right)$$

$\longrightarrow$ The $\mathcal{C}_x$'s are orthogonal: it defines a projective measurement!

(II) Fundamental idea: syndrome measurement

Measure according to Eq. (1). Then apply **X** on a qubit according to the result x. For instance:

$0 \mapsto$ do nothing, $\quad 1 \mapsto$ apply **X** on the first qubit, $\quad 2 \mapsto$ apply **X** on the second qubit, etc

But why does it work?

(I) Fundamental idea: decompose the three qubits space as (coset decomposition)

$$\left(\mathbb{C}^2\right)^{\otimes 3} = \mathcal{C}_0 \overset{\perp}{\oplus} \mathcal{C}_1 \overset{\perp}{\oplus} \mathcal{C}_2 \overset{\perp}{\oplus} \mathcal{C}_3 \tag{1}$$

where,

$$\mathcal{C}_0 \overset{\text{def}}{=} \text{Vect}\left(|000\rangle, |111\rangle\right), \quad \mathcal{C}_1 \overset{\text{def}}{=} \text{Vect}\left(|100\rangle, |011\rangle\right), \quad \mathcal{C}_2 \overset{\text{def}}{=} \text{Vect}\left(|010\rangle, |101\rangle\right)$$

$$\mathcal{C}_3 \overset{\text{def}}{=} \text{Vect}\left(|001\rangle, |110\rangle\right)$$

$\longrightarrow$ The $\mathcal{C}_x$'s are orthogonal: it defines a projective measurement!

(II) Fundamental idea: syndrome measurement

Measure according to Eq. (1). Then apply $\mathbf{X}$ on a qubit according to the result x. For instance:

$0 \mapsto$ do nothing, $\quad 1 \mapsto$ apply $\mathbf{X}$ on the first qubit, $\quad 2 \mapsto$ apply $\mathbf{X}$ on the second qubit, etc

But why does it work?

If one error $\mathbf{X}$ occurred, the quantum state will belong with certainty to some $\mathcal{C}_x$ and $\mathbf{X}^2 = \mathbf{I}_2$

Error X on the second qubit:

$$\alpha |000\rangle + \beta |111\rangle \rightsquigarrow \alpha |010\rangle + \beta |101\rangle$$

- Measure according to the orthogonal projections over

$$\mathcal{C}_0 = \text{Vect}\left(|000\rangle, |111\rangle\right), \quad \mathcal{C}_1 = \text{Vect}\left(|100\rangle, |011\rangle\right), \quad \mathcal{C}_2 = \text{Vect}\left(|010\rangle, |101\rangle\right)$$
$$\mathcal{C}_3 = \text{Vect}\left(|001\rangle, |110\rangle\right)$$

- With probability one we measure 2 $\left(\text{“we are in } \mathcal{C}_2\text{”}\right)$ and the quantum state does not change

$$\alpha |010\rangle + \beta |101\rangle$$

- Apply **X** on the second qubit

$$\alpha |010\rangle + \beta |101\rangle \longmapsto \alpha |000\rangle + \beta |111\rangle$$

Remarkable fact:

Measurement does not change the quantum state!

Error of type-X on some "random qubit":

$$\alpha\,|000\rangle + \beta\,|111\rangle \rightsquigarrow a\,(\alpha\,|100\rangle + \beta\,|011\rangle) + b\,(\alpha\,|010\rangle + \beta\,|101\rangle) + c\,(\alpha\,|001\rangle + \beta\,|110\rangle)$$

Same decoding algorithm: measure according to $\mathcal{C}_0 \overset{\perp}{\oplus} \mathcal{C}_1 \overset{\perp}{\oplus} \mathcal{C}_2 \overset{\perp}{\oplus} \mathcal{C}_3$ but this times the quantum states changes

- With probability $|a|^2$ observe "error on the first qubit", the quantum state collapses to

  $$\alpha\,|100\rangle + \beta\,|011\rangle$$

  and apply **X** on the first qubit,
- With probability $|b|^2$ observe "error on the second qubit", the quantum state collapses to

  $$\alpha\,|010\rangle + \beta\,|101\rangle$$

  and apply **X** on the second qubit,
- etc. . .

What is the most important sentence of MDC_51002_EP $\left(\textit{first semester course}\right)$*?*

What is the most important sentence of MDC_51002_EP $\Big($*first semester course*$\Big)$*?*

Quantum computation offers you a huge power with the “-1”

It is the same for errors, errors have a huge power, phase-flip can happen **Z** : $\begin{cases} |0\rangle \mapsto & |0\rangle \\ |1\rangle \mapsto & -|1\rangle \end{cases}$

*But is our previous quantum code with its decoding algorithm useful against errors of type-***Z***?*

$\longrightarrow$ No!

Applying Z on some qubit:

$$\alpha\,|000\rangle - \beta\,|111\rangle$$

- Decoding: measuring leads to we are in $\mathcal{C}_0$: “no error” and we do nothing. . .

Fundamental remark:

errors of type **Z** $\equiv$ errors of type **X** in the Fourier basis $|+\rangle, |-\rangle$

$$\mathsf{Z} : \begin{cases} |+\rangle \mapsto |-\rangle \\ |-\rangle \mapsto |+\rangle \end{cases} \quad \text{and} \quad \mathsf{X} : \begin{cases} |+\rangle \mapsto \ \ |+\rangle \\ |-\rangle \mapsto -|-\rangle \end{cases}$$

Natural idea: apply $\mathsf{H}^{\otimes 3}$ to $\alpha |000\rangle + \beta |111\rangle$:

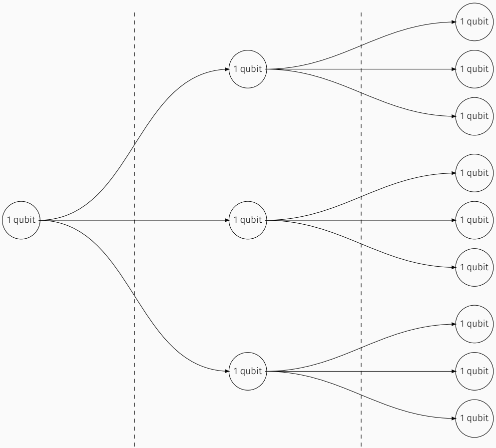
$$\alpha |+++\rangle + \beta |---\rangle$$

As above we can correct any error of type **Z** on one qubit with this encoding!

$\longrightarrow$ But we are stuck, we cannot correct errors of type-**X** anymore. . .

Idea: concatenation trick

Encode to protect against **Z**-errors and then encode this to protect against **X**-errors!



Protection against **Z**-errors   Protection against **X**-errors

$$|0\rangle \xrightarrow{\textit{1st}} |+++\rangle = \frac{1}{2\sqrt{2}}(|0\rangle + |1\rangle)^{\otimes 3} \xrightarrow{\textit{2nd}} \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)^{\otimes 3}$$

$$|1\rangle \xrightarrow{\textit{1st}} |---\rangle = \frac{1}{2\sqrt{2}}(|0\rangle - |1\rangle)^{\otimes 3} \xrightarrow{\textit{2nd}} \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)^{\otimes 3}$$

- 1st step: protecting against errors of type-**Z**
- 2nd step: protecting against errors of type-**X**

Encoding:

$$\left(\alpha |0\rangle + \beta |1\rangle\right) \otimes \left|0^8\right\rangle \longmapsto \frac{\alpha}{2\sqrt{2}}(|000\rangle + |111\rangle)^{\otimes 3} + \frac{\beta}{2\sqrt{2}}(|000\rangle - |111\rangle)^{\otimes 3}$$

$$\frac{\alpha}{2\sqrt{2}}\left(|000\rangle + |111\rangle\right)^{\otimes 3} + \frac{\beta}{2\sqrt{2}}\left(|000\rangle - |111\rangle\right)^{\otimes 3}$$

$\longrightarrow$ The encoding belongs to the linear code $\mathcal{C}$ of dimension 3 generated by

(111000000), (000111000), (000000111)

As previously, one can define the syndrome measurement according to the cosets:

$$\mathcal{C}_0 \stackrel{\text{def}}{=} \text{Vect}\left(|\mathbf{x}\rangle \ : \ \mathbf{x} \in \mathcal{C}\right), \mathcal{C}_1 \stackrel{\text{def}}{=} \text{Vect}\left(|\mathbf{x} + (1,0,0,0,0,0,0,0,0)\rangle \ \ \mathbf{x} \in \mathcal{C}\right), \quad \text{etc}\ldots$$

$\longrightarrow$ 9 subspaces of dimension 3 in orthogonal sum! It defines a (syndrome) measurement

enabling, as previously, to correct any one X-error

Remark:

This syndrome measurement: any interference with any possible **Z**-error

(change signs not switch vectors of the computational basis)

Once we have removed a possible **X**-error we are left to deal with

$$\frac{\alpha}{2\sqrt{2}}\left(|000\rangle+|111\rangle\right)^{\otimes 3}+\frac{\beta}{2\sqrt{2}}\left(|000\rangle-|111\rangle\right)^{\otimes 3}=\alpha\,|+_3+_3+_3\rangle+\beta\,|-_3-_3-_3\rangle$$

$$|+_3\rangle \stackrel{\text{def}}{=} \frac{|000\rangle+|111\rangle}{\sqrt{2}} \quad \text{and} \quad |-_3\rangle \stackrel{\text{def}}{=} \frac{|000\rangle-|111\rangle}{\sqrt{2}}$$

$\longrightarrow$ **One** **Z**-error on any qubit of $|+_3\rangle$ leads to $|-_3\rangle$!

Z-error on either 1st, 2nd or 3rd $\left(\textit{resp.}\ \text{4th, 5th or 6th}\right)$ qubit yields:

$$\alpha\,|-_3+_3+_3\rangle+\beta\,|+_3-_3-_3\rangle \quad \left(\textit{resp.}\ \alpha\,|+_3-_3+_3\rangle+\beta\,|-_3+_3-_3\rangle\right)$$

- We can define the syndrome measurement: $\left(\mathbb{C}^2\right)^{\otimes 9}=\mathcal{E}_0\overset{\perp}{\oplus}\mathcal{E}_1\overset{\perp}{\oplus}\mathcal{E}_2\overset{\perp}{\oplus}\mathcal{E}_3\overset{\perp}{\oplus}F$ where:

$$\mathcal{E}_0 \stackrel{\text{def}}{=} \mathrm{Vect}\left(|+_3+_3+_3\rangle,|-_3-_3-_3\rangle\right),\ \mathcal{E}_1 \stackrel{\text{def}}{=} \mathrm{Vect}\left(|-_3+_3+_3\rangle,|+_3-_3-_3\rangle\right),\ \dots,\ F \stackrel{\text{def}}{=} \left(\sum_i \mathcal{E}_i\right)^{\perp}$$

Decoding:

Measure $\left(\text{it does not change the quantum state}\right)$ and then apply **Z** on the either the 1st, 2nd or 3rd qubit if the answer is 1, etc...

Shor's quantum error correcting code:

It can correct one error of type-X and one error of type-Z!

Exercise:

Find an error on two qubits which cannot be corrected by Shor's code

- Are the errors of type-X and Z be the only possible errors?
- Can Shor's quantum code correct these other potential errors?

$\longrightarrow$ As in classical world: many reasonable models of errors

But there is a moral:

Errors on qubits: apply Pauli matrices

Single qubit Pauli group $\mathcal{P}_1$:

$$\{\pm I_2, \pm X, \pm Y, \pm Z, \pm iI_2, \pm iX, \pm iY, \pm iZ\}$$

$\longrightarrow$ This set **forms a group** for the multiplication!

- $X^2 = Y^2 = Z^2 = I_2$
- The $\neq$ Pauli matrices anti-commute: $XZ = -ZX = -iY$ etc. . .

Exercise Session:

Any 2×2 matrix M on one qubit can be written as:

$$M = e_0 I_2 + e_1 X + e_2 Z + e_3 XZ$$

One reasonable model of error: on each qubit we independently apply a linear operator

Any linear operator **M** on one qubit can be written as:

$$\mathbf{M} = e_0\mathbf{I}_2 + e_1\mathbf{X} + e_2\mathbf{Z} + e_3\mathbf{XZ}$$

$\longrightarrow$ We reduce a continuous set of errors to a discrete set of errors given by **X**, **Z** and **XZ**

Correcting a discrete set of errors by syndrome measurement: **X** and **Z**

$\longrightarrow$ We can automatically correct a much larger $\big($continuous!$\big)$ class of errors

Intuitively: if the syndrome measurement is correct with certainty, performing this measurement after applying **M** will collapse the quantum state into no error, error of type-**X** and **Z**

Shor's code can correct all errors of type **X** and **Z**!

Depolarizing channel:

Each qubit independently undergoes an error X, Z or $Y = iXZ$ with probability $p/3$ and is not modified with probability p

On a single qubit, in terms of density operator:

$$\rho \longmapsto \mathcal{E}(\rho) \stackrel{\text{def}}{=} (1-p)\rho + \frac{p}{3}X\rho X + \frac{p}{3}Y\rho Y + \frac{p}{3}Z\rho Z$$

$\longrightarrow$ Somehow the quantum analogue of the Binary Symmetric channel

Exercise:

Show that when $p = \frac{3}{4}$, then $\mathcal{E}(\rho) = \frac{I_2}{2}$. How do you interpret this result? What would be the "classical" equivalent with the Binary Symmetric Channel?

Quantum channels:

It belongs to a more general theory: quantum measurements, Krauss operators

Errors against which we need to be protected:

X and Z

Decoding Shor's quantum code:

Shor's quantum code can correct any $\big($continuous$\big)$ error provided they only affect a single qubit

$\longrightarrow$ But to protect one qubit we need nine qubits...

Can we do better?

$\longrightarrow$ Yes, let's go! But before break...

CSS CODES

We study now Calderbank-Shor-Steane (CSS) codes

Aim:

A more systematic way of encoding quantum states using (classical) linear codes

CSS construction is based on two classical codes:

- the first one corrects errors of type-**X**
- the second one corrects errors of type-**Z**

For any $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_2^n$,

$$\mathsf{X}^{\mathbf{v}} \stackrel{\text{def}}{=} \mathsf{X}^{v_1} \otimes \mathsf{X}^{v_2} \otimes \cdots \otimes \mathsf{X}^{v_n} \quad \text{and} \quad \mathsf{Z}^{\mathbf{v}} \stackrel{\text{def}}{=} \mathsf{Z}^{v_1} \otimes \mathsf{Z}^{v_2} \otimes \cdots \otimes \mathsf{Z}^{v_n}$$

Lemma:

(*i*) $\mathsf{X}^{\mathbf{u}}\mathsf{Z}^{\mathbf{v}} = (-1)^{\langle \mathbf{u},\mathbf{v}\rangle}\mathsf{Z}^{\mathbf{v}}\mathsf{X}^{\mathbf{u}}$

(*ii*) $\mathsf{H}^{\otimes n}\mathsf{X}^{\mathbf{u}} = \mathsf{Z}^{\mathbf{u}}\mathsf{H}^{\otimes n}$ and $\mathsf{H}^{\otimes n}\mathsf{Z}^{\mathbf{u}} = \mathsf{X}^{\mathbf{u}}\mathsf{H}^{\otimes n}$

(*iii*) $\mathsf{Z}^{\mathbf{u}} |\mathbf{x}\rangle = (-1)^{\langle \mathbf{u},\mathbf{x}\rangle} |\mathbf{x}\rangle$

Proof:

Consequence of the fact that $\mathsf{XZ} = -\mathsf{ZX}$ and $\mathsf{XH} = \mathsf{HZ}$

Lemma:

For any linear code $\mathcal{C}$,

$$\mathsf{H}^{\otimes n}\left|\mathcal{C}\right\rangle = \left|\mathcal{C}^{\perp}\right\rangle \quad \text{where } \left|\mathcal{C}\right\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{\sharp\mathcal{C}}}\sum_{\mathbf{c}\in\mathcal{C}}\left|\mathbf{c}\right\rangle \quad \text{and} \quad \left|\mathcal{C}^{\perp}\right\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{\sharp\mathcal{C}^{\perp}}}\sum_{\mathbf{c}^{\perp}\in\mathcal{C}^{\perp}}\left|\mathbf{c}^{\perp}\right\rangle$$

Proof:

See Exercise Session

But from which result this lemma comes from?

Lemma:

For any linear code $\mathcal{C}$,

$$\mathsf{H}^{\otimes n} |\mathcal{C}\rangle = \left|\mathcal{C}^{\perp}\right\rangle \quad \text{where} \quad |\mathcal{C}\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{\sharp \mathcal{C}}} \sum_{\mathbf{c} \in \mathcal{C}} |\mathbf{c}\rangle \quad \text{and} \quad \left|\mathcal{C}^{\perp}\right\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{\sharp \mathcal{C}^{\perp}}} \sum_{\mathbf{c}^{\perp} \in \mathcal{C}^{\perp}} \left|\mathbf{c}^{\perp}\right\rangle$$

Proof:

See Exercise Session

But from which result this lemma comes from?

$\longrightarrow$ Poisson summation formula

- Defined from two linear codes $\left(\mathcal{C}_X, \mathcal{C}_Z\right)$ of length n such that $\mathcal{C}_Z \subseteq \mathcal{C}_X \subseteq \mathbb{F}_2^n$

$$k \stackrel{\text{def}}{=} \dim \mathcal{C}_X/\mathcal{C}_Z = \dim \mathcal{C}_X - \dim \mathcal{C}_Z$$

$\longrightarrow \mathcal{C}_X = \bigsqcup_{1\leq i\leq 2^k} (\mathbf{x}_i + \mathcal{C}_Z)$ for 2^k vectors $\mathbf{x}_i \in \mathcal{C}_X$ being coset representatives of $\mathcal{C}_X/\mathcal{C}_Z$

There are efficient one-to-one mappings:

$$\mathbf{i} \in \{0,1\}^k \longmapsto \mathbf{x}_i \in \{0,1\}^n \quad \text{and} \quad \mathbf{x}_i \in \{0,1\}^n \longmapsto \mathbf{i} \in \{0,1\}^k$$

CSS quantum codes:

CSS codes encodes k qubits as

$$\sum_{\mathbf{i}\in\{0,1\}^k} \alpha_{\mathbf{i}} \underbrace{|\mathbf{i}\rangle}_{k \text{ qubits}} \otimes \left|0^{n-k}\right\rangle \longmapsto \sum_{\mathbf{x}_i} \alpha_{\mathbf{i}} \underbrace{|\mathbf{x}_i + \mathcal{C}_Z\rangle}_{n \text{ qubits}}$$

where,
$$|\mathbf{x} + \mathcal{C}_Z\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{\sharp \mathcal{C}_Z}} \sum_{\mathbf{y}\in\mathcal{C}_Z} |\mathbf{x}+\mathbf{y}\rangle$$

Exercise session:

How to efficiently build CSS encodings?

⟶ As for Shor's code, use: syndrome measurement

Syndrome measurement:

Let $\mathcal{C}$ be a linear code of length n, dimension k and with parity-check matrix $\mathbf{H}$.

We associate to $\mathcal{C}$ and $\mathbf{H}$ the following measurement

$$\left(\mathbb{C}^2\right)^{\otimes n} = \bigoplus_{\mathbf{s}\in\mathbb{F}_2^{n-k}}^{\perp} \mathcal{E}_{\mathbf{s}}^{\mathcal{C}}$$

where,

$$\mathcal{E}_{\mathbf{s}}^{\mathcal{C}} \stackrel{\text{def}}{=} \text{Vect}\left(\underbrace{|\mathbf{z}\rangle}_{n \text{ qubits}} : \mathbf{H}\mathbf{z}^{\mathsf{T}} = \mathbf{s}^{\mathsf{T}}\right) = \text{Vect}\left(|\mathbf{z}\rangle : \mathbf{z} \in \mathbf{x} + \mathcal{C} \text{ where } \mathbf{H}\mathbf{x}^{\mathsf{T}} = \mathbf{s}^{\mathsf{T}}\right)$$

⟶ The $\mathcal{E}_{\mathbf{s}}^{\mathcal{C}}$'s are generated by the vectors of different cosets

But as the cosets are disjoint, the $\mathcal{E}_{\mathbf{s}}^{\mathcal{C}}$'s are orthogonal!

A crucial remark:

If $|\psi\rangle \in \mathcal{E}_{0}^{\mathcal{C}}$, then $\mathbf{X}^{\mathbf{e}}\,|\psi\rangle \in \mathcal{E}_{\mathbf{s}}^{\mathcal{C}}$ where $\mathbf{H}\mathbf{e}^{\mathsf{T}} = \mathbf{s}^{\mathsf{T}}$

⟶ If the $\mathbf{H}\mathbf{e}_i^{\mathsf{T}}$'s are distinct and we can recover $\mathbf{e}_i$ from $\mathbf{H}\mathbf{e}_i^{\mathsf{T}}$: when measuring $\mathbf{X}^{\mathbf{e}_i}\,|\psi\rangle \in \mathcal{E}_{\mathbf{H}\mathbf{e}_i^{\mathsf{T}}}^{\mathcal{C}}$ we recover $\mathbf{H}\mathbf{e}_i^{\mathsf{T}}$, then $\mathbf{e}_i$ and we can remove $\mathbf{X}^{\mathbf{e}_i}$

$$\left(|x + \mathcal{C}\rangle = \frac{1}{\sqrt{\sharp \mathcal{C}}} \sum_{c \in \mathcal{C}} |x + c\rangle \right)$$

Starting from the encoding and applying the noise $X^e Z^f$:

$$|\psi\rangle = \sum_{x \in \mathcal{C}_X / \mathcal{C}_Z} \alpha_x |x + \mathcal{C}_Z\rangle \in \mathcal{E}_0^{\mathcal{C}_X} \rightsquigarrow X^e Z^f |\psi\rangle = \sum_{x \in \mathcal{C}_X / \mathcal{C}_Z} \alpha_x X^e Z^f |x + \mathcal{C}_Z\rangle$$

$\longrightarrow$ Z^f only modifies signs! Therefore:

$$\sum_{x \in \mathcal{C}_X / \mathcal{C}_Z} \alpha_x X^e Z^f |x + \mathcal{C}_Z\rangle \in \mathcal{E}_{H_X e^T}^{\mathcal{C}_X} \quad \text{where } H_X \text{ be a parity-check matrix of } \mathcal{C}_X \supseteq \mathcal{C}_Z$$

$$\left(\text{because:} \quad \forall x \in \mathcal{C}_X, c_Z \in \mathcal{C}_Z, \quad H_X(x + c_Z)^T = 0 \quad \text{as } x \in \mathcal{C}_X \quad \text{and} \quad c_Z \in \mathcal{C}_Z \subseteq \mathcal{C}_X\right)$$

Syndrome measurement:

It does not modify the quantum state, supposing that we can recover $\mathbf{e}$ from $H_X \mathbf{e}^T$: remove X^e

$$|\psi\rangle = \sum_{x \in \mathcal{C}_X/\mathcal{C}_Z} \alpha_x |x + \mathcal{C}_Z\rangle \in \mathcal{E}_0^{\mathcal{C}_X} \rightsquigarrow X^e Z^f |\psi\rangle \xrightarrow{\text{1st decoding}} Z^f |\psi\rangle = \sum_{x \in \mathcal{C}_X/\mathcal{C}_Z} \alpha_x Z^f |x + \mathcal{C}_Z\rangle$$

Fundamental remark:

We have the following identities:

$$Z^f |\psi\rangle = \sum_{x \in \mathcal{C}_X/\mathcal{C}_Z} \alpha_x Z^f |x + \mathcal{C}_Z\rangle = \sum_{x \in \mathcal{C}_X/\mathcal{C}_Z} \alpha_x Z^f X^x |\mathcal{C}_Z\rangle$$

By applying $H^{\otimes n}$:

$$\begin{aligned} H^{\otimes n} Z^f |\psi\rangle &= \sum_{x \in \mathcal{C}_X/\mathcal{C}_Z} \alpha_x H^{\otimes n} Z^f X^x |\mathcal{C}_Z\rangle \\ &= \sum_{x \in \mathcal{C}_X/\mathcal{C}_Z} \alpha_x X^f Z^x H^{\otimes n} |\mathcal{C}_Z\rangle \\ &= X^f \sum_{x \in \mathcal{C}_X/\mathcal{C}_Z} \alpha_x Z^x \left|\mathcal{C}_Z^\perp\right\rangle \in \text{in the coset given by } \mathbf{H}_Z \mathbf{f}^\top \text{ with } \mathbf{H}_Z \text{ parity-check of } \mathcal{C}_Z^\perp \end{aligned}$$

Syndrome measurement with $\mathcal{C}_Z^\perp$:

Measuring: we can recover **f**, then we apply $H^{\otimes n}$ leading to $Z^f |\psi\rangle$ and we remove Z^f

Up to now we used the fact that we can "decode" $\mathcal{C}_X$ and $\mathcal{C}_Z^{\perp}$

Let, $\mathbf{H}_X$ and $\mathbf{H}_Z$ be a parity-check matrix of $\mathcal{C}_X$ and $\mathcal{C}_Z^{\perp}$

- To remove errors $X^{\mathbf{e}_1}$, or $X^{\mathbf{e}_2}$, . . . , or $X^{\mathbf{e}_\ell}$:

  the $\mathbf{H}_X\mathbf{e}_i^{\mathsf{T}}$'s have to be distinct and we can efficiently recover $\mathbf{e}_j$ from $\mathbf{H}_X\mathbf{e}_j^{\mathsf{T}}$

- To remove errors $Z^{\mathbf{f}_1}$, or $Z^{\mathbf{f}_2}$, . . . , or $Z^{\mathbf{f}_\ell}$:

  the $\mathbf{H}_Z\mathbf{f}_i^{\mathsf{T}}$'s have to be distinct and we can efficiently recover $\mathbf{f}_j$ from $\mathbf{H}_Z\mathbf{f}_j^{\mathsf{T}}$

But, can we find classical codes offering such "properties"?

$\longrightarrow$ Yes! To understand why it is theoretically possible: minimum distance

Hamming weight:

$$\forall \mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{F}_2^n, \quad |\mathbf{x}| \stackrel{\text{def}}{=} \sharp \{i \in [\![1, n]\!], \ x_i \neq 0\}$$

Minimum distance:

Let $\mathcal{C} \subseteq \mathbb{F}_2^n$ (linear code), its minimum distance is defined as

$$d_{\text{min}}(\mathcal{C}) \stackrel{\text{def}}{=} \min \{|\mathbf{c}| \ : \ \mathbf{c} \in \mathcal{C} \text{ and } \mathbf{c} \neq \mathbf{0}\}$$

$\longrightarrow$ The minimum distance quantifies how “good” is a code in terms of decoding ability!

Lemma (see previous exercise session):

Let $\mathbf{H}$ be any parity-check matrix of $\mathcal{C}$, then

the $\mathbf{H}\mathbf{e}^{\mathsf{T}}$'s are distinct **when** $|\mathbf{e}| < \frac{d_{\text{min}}(\mathcal{C})}{2}$

$\longrightarrow$ $\mathcal{C}$ can theoretically be decoded if there are $< \frac{d_{\text{min}}(\mathcal{C})}{2}$ errors

Be careful: it does not show the existence of an efficient decoding algorithm, which is far from being guaranteed

- What is the best minimum distance can we expect?

  $\longrightarrow$ It is typically large $\approx n/10$ when $\mathcal{C}$ has dimension $n/2$ $\left(\text{see previous exercise session}\right)$

- Do we know linear codes with a large minimum distance and for which we can remove a large number of errors?

  $\longrightarrow$ Hard question... Yes we can $\left(\text{hopefully for telecommunication}\right)$ but to understand how deserves at least other lectures...

To take away:

It exists codes with a large minimum distance d and we can hope to be able to decode up to $d/2$

But: hard to find codes with a large d and for which we can efficiently decode many errors $\left(\text{even} \ll d/2\right)$

$\longrightarrow$ Active research topic with a lot a consequences, event recent $\left(\text{for instance the 5}G\ldots\right)$

To build CSS codes: choose $\mathcal{C}$ such that (i) can correct many errors and (ii) $\mathcal{C}^{\perp} \subseteq \mathcal{C}$ $\left(\text{weekly auto-dual}\right)$

Theorem: decoding CSS codes

Let $\mathcal{C}_\mathsf{X}$ and $\mathcal{C}_\mathsf{Z}$ be linear codes such that $\mathcal{C}_\mathsf{Z} \subseteq \mathcal{C}_\mathsf{X}$

If $\mathbf{e}$ $\left(\textit{resp. } \mathbf{f}\right)$ can be recovered from its syndrome by the code $\mathcal{C}_\mathsf{X}$ $\left(\textit{resp. } \mathcal{C}_\mathsf{Z}^\perp\right)$, then the quantum error pattern $\mathsf{X}^{\mathbf{e}}\mathsf{Z}^{\mathbf{f}}$ can be corrected by the CSS quantum code associated to the pair $\left(\mathcal{C}_\mathsf{X}, \mathcal{C}_\mathsf{Z}\right)$

In particular, we can hope to decode up to $d_{\min}(\mathcal{C}_\mathsf{X})/2$ errors-X and $d_{\min}(\mathcal{C}_\mathsf{Z}^\perp)/2$ errors-Z (even combined)

See Exercise Session:

- Shor's code (9 qubits to protect 1 qubit) is a CSS code
- Steane's code (7 qubits to protect 1 qubit) is a CSS code using Hamming codes

STABILIZER CODES

- A class of codes containing CSS codes
- Many similarities with classical linear codes
- Powerful framework for defining/manipulating/constructing/understanding quantum codes

$$\begin{aligned} XZ &= -ZX &= -iY \\ XY &= -YX &= iZ \\ YZ &= -ZY &= iX \end{aligned}$$

$\longrightarrow$ The elements of $\mathbb{G}_1 = \{\pm 1, \pm i\} \times \{X, Z, Y\}$ commute or anti-commute

$\mathbb{G}_n$-group:

The set of operators of the form $\pm X^{\mathbf{e}} Z^{\mathbf{f}}$ or $\pm i X^{\mathbf{e}} Z^{\mathbf{f}}$, where $\mathbf{e}, \mathbf{f} \in \mathbb{F}_2^n$, form a multiplicative group

Admissible subgroup:

A subgroup $\mathbb{S}$ of $\mathbb{G}_n$ is said to be admissible if: $-\mathbf{I}^{\otimes n} \notin \mathbb{S}$

$\longrightarrow$ We will only consider admissible subgroups!

Lemma:

Any admissible subgroup $\mathbb{S}$ is Abelian $\Big($its elements commute$\Big)$

Proof:

Let $\mathbf{E}, \mathbf{F} \in \mathbb{S} \subseteq \mathbb{G}_n$, then

$$\mathbf{E}^2 = \pm\mathbf{I}, \quad \mathbf{F}^2 = \pm\mathbf{I} \quad \text{and} \quad \mathbf{EF} = \pm\mathbf{FE}$$

But $\mathbf{E}^2, \mathbf{F}^2 \in \mathbb{S}$ and $-\mathbf{I} \notin \mathbb{S}$. Therefore:

$$\mathbf{E}^2 = \mathbf{F}^2 = \mathbf{I}$$

Suppose by contradiction that $\mathbf{EF} = -\mathbf{FE}$, then

$$\mathbf{EFEF} = -\mathbf{EF}^2\mathbf{E} = -\mathbf{I} \in \mathbb{S}\text{: contradiction}$$

Stabilizer code:

$\mathbb{S}$ be an admissible subgroup of $\mathbb{G}_n$

The **stabilizer code** $\mathcal{C}$ associated to $\mathbb{S}$ is defined as

$$\mathcal{C} \stackrel{\text{def}}{=} \left\{ |\psi\rangle : \forall \mathsf{M} \in \mathbb{S}, \; \mathsf{M}\,|\psi\rangle = |\psi\rangle \right\}$$

An example:

$\mathrm{Vect}\left(|000\rangle, |111\rangle\right)$ is a stabilizer code associated to

$$\left\{ \mathsf{I} \otimes \mathsf{I} \otimes \mathsf{I}, \; \mathsf{Z} \otimes \mathsf{Z} \otimes \mathsf{I}, \; \mathsf{Z} \otimes \mathsf{I} \otimes \mathsf{Z}, \; \mathsf{I} \otimes \mathsf{Z} \otimes \mathsf{Z} \right\}$$

Given $\mathbb{S}$ an admissible subgroup of $\mathbb{G}_n$:

- **Generators set**: $\mathsf{M}_1, \ldots, \mathsf{M}_\ell$ such that

$$\forall \mathsf{M} \in \mathbb{S}, \; \mathsf{M} = \mathsf{M}_1^{e_1} \cdots \mathsf{M}_\ell^{e_\ell} \;\text{ for }\; e_1, \ldots, e_\ell \in \{0,1\}$$

Notation:

$$\langle \mathsf{M}_1, \ldots, \mathsf{M}_\ell \rangle \stackrel{\text{def}}{=} \left\{ \mathsf{M}_1^{e_1} \cdots \mathsf{M}_\ell^{e_\ell} \;\text{ for }\; e_1, \ldots, e_\ell \in \{0,1\} \right\}$$

- **Minimal generators set** $\Big($independent generators in the literature$\Big)$: $\mathsf{M}_1, \ldots, \mathsf{M}_\ell$ such that

$$\forall i, \quad \langle \mathsf{M}_1, \ldots, \mathsf{M}_{i-1}, \mathsf{M}_{i+1}, \ldots, \mathsf{M}_\ell \rangle \subsetneq \langle \mathsf{M}_1, \ldots, \mathsf{M}_\ell \rangle$$

Proposition $\Big($admitted$\Big)$:

$\mathbb{S}$ admits a minimal generator set $\mathsf{M}_1, \ldots, \mathsf{M}_r$ for some r and

$$\sharp\mathbb{S} = 2^r$$

$\mathbb{S} \subseteq \mathbb{G}_n$ admissible subgroup

$\sharp\mathbb{S} = 2^r$ and $\mathbf{M}_1, \ldots, \mathbf{M}_r$ minimal set of generators

The syndrome function:

$$\sigma : \mathbb{G}_n \longrightarrow \{0,1\}^r$$

$$\mathbf{E} \longmapsto \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_r \end{pmatrix} \quad \text{with} \quad s_i \stackrel{\text{def}}{=} \begin{cases} 0 & \text{if } \mathbf{E}\mathbf{M}_i = \mathbf{M}_i\mathbf{E} \\ 1 & \text{if } \mathbf{E}\mathbf{M}_i = -\mathbf{M}_i\mathbf{E} \end{cases}$$

Remark:

For any $\mathbf{M} \in \mathbb{S}$: $\sigma(\mathbf{M}) = \mathbf{0}$

$$\text{Syndrome: } \sigma(\mathsf{E}) = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_r \end{pmatrix} \quad \text{with } s_i \stackrel{\text{def}}{=} \begin{cases} 0 & \text{if } \mathsf{EM}_i = \mathsf{M}_i\mathsf{E} \\ 1 & \text{if } \mathsf{EM}_i = -\mathsf{M}_i\mathsf{E} \end{cases}$$

$$\mathcal{C}(\mathsf{s}) \stackrel{\text{def}}{=} \left\{ |\psi\rangle\,,\ \forall i,\ \mathsf{M}_i\,|\psi\rangle = (-1)^{s_i}\,|\psi\rangle \right\}$$

$$\longrightarrow \mathcal{C}(0) = \mathcal{C}$$

Proposition (admitted): a quantum measurement that extracts the syndrome

1. For any $\mathbf{E} \in \mathbb{G}_n$ and any $|\psi\rangle \in \mathcal{C}$:
$$\mathsf{E}\,|\psi\rangle \in \mathcal{C}(\sigma(\mathsf{E}))$$
2. $\left(\mathbb{C}^2\right)^{\otimes n}$ decomposes into the orthogonal direct sum:
$$\left(\mathbb{C}^2\right)^{\otimes n} = \bigoplus_{\mathsf{s}\in\mathbb{F}_2^r}^{\perp} \mathcal{C}(\mathsf{s})$$

$$\longrightarrow \text{The } \mathcal{C}(\mathbf{s})\text{'s define a measurement!}$$

Proposition (admitted):

For any $\mathbf{s} \in \mathbb{F}_2^r$, there exists $\mathbf{E} \in \mathbb{G}_n$ such that $\mathbf{s} = \sigma(\mathsf{E})$

We have $\dim_{\mathbb{C}}(\mathcal{C}) = 2^{n-r}$

Linear codes	Stabilizer codes
k bits encoded in n bits subspace of dimension k	k qubits encoded in n qubits subspace of dimension 2^k
parity-check matrix $\mathbf{H}$ $r = n - k$ rows, n columns syndrome $\in \{0,1\}^{n-k}$	minimal generators set of $\mathbb{S}$ $r = n - k$ generators syndrome $\in \{0,1\}^{n-k}$

Error: $\mathsf{E} \in \mathbb{G}_n$

$$|\psi\rangle \in \mathcal{C} \rightsquigarrow \mathsf{E}\,|\psi\rangle \in \mathcal{C}(\sigma(\mathsf{E})) \xrightarrow{\text{measurement}} \mathsf{E}\,|\psi\rangle \text{ with the knowledge of } \sigma(\mathsf{E})$$

- But how to extract **E**?

  $\longrightarrow$ classically

- What are the errors that can be corrected?

  $\longrightarrow$ Subtle question!

Suppose: $|\psi\rangle \rightsquigarrow \mathbf{E}|\psi\rangle$ where $\mathbf{E} \in \mathbb{G}_n$

$\longrightarrow$ We want to remove $\mathbf{E}$, *i.e.*, to apply $\mathbf{E}^{-1}$

Decoding process:

We compute $\mathbf{E}' \in \mathbb{G}_n$ such that $\mathbf{E}'\mathbf{E}|\psi\rangle \in \mathcal{C} = \mathcal{C}(\mathbf{0})$. In other words,

$$\sigma(\mathbf{E}\mathbf{E}') = 0$$

Is $\mathbf{E}' = \mathbf{E}^{-1}$? Is it necessary?

$\longrightarrow$ We don't need $\mathbf{E} = \mathbf{E}^{-1}$, we only need $\mathbf{E}'\mathbf{E}|\psi\rangle = |\psi\rangle$

Suppose: $|\psi\rangle \rightsquigarrow \mathbf{E}\,|\psi\rangle \in \mathcal{C}(\mathbf{0}) = \mathcal{C} \xrightarrow{\textit{measurement}}$ syndrome **0**, no error...

Is it a problem? It depends of **E**... Is $\mathbf{E}\,|\psi\rangle = |\psi\rangle$ or not?

We can distinguish two types of error E with syndrome 0:

- Harmless error $\Big($type-**G** like "Good"$\Big)$: $\mathbf{E} \in \mathbb{S}$, in that case

$$\forall\,|\psi\rangle \in \mathcal{C}, \quad \mathbf{E}\,|\psi\rangle = |\psi\rangle$$

- Harmful error $\Big($type-**B** like "Bad"$\Big)$: $\mathbf{E} \notin \mathbb{S}$, in that case $\Big($proof: use the "minimality" of generators$\Big)$

$$\exists\,|\psi\rangle \in \mathcal{C}, \quad \mathbf{E}\,|\psi\rangle \neq |\psi\rangle$$

Type-**B** errors: cannot be detected and thus cannot be corrected while it may happen $\mathbf{E}\,|\psi\rangle \neq |\psi\rangle$

To overcome this issue: introduce the minimum distance

Remark:

An harmful error **E** verifies by definition $\sigma(\mathbf{E}) = \mathbf{0}$

Recall: if $\mathsf{E} \in \mathbb{G}_n$, then $\mathsf{E} = \mathsf{X}^{\mathbf{e}}\mathsf{Z}^{\mathbf{f}} \left(\text{up to } \times\{\pm 1, \pm i\}\right)$ for some $\mathbf{e}, \mathbf{f} \in \mathbb{F}_2^n$,

Weight Pauli group elements:

For any $\mathsf{E} \in \mathbb{G}_n$, we define its weight as,

$$|\mathsf{E}| \stackrel{\text{def}}{=} \sharp\left\{i : e_i \neq f_i \text{ or } e_i = f_i = 1\right\} = \sharp\left\{\mathsf{X}, \mathsf{Y}, \mathsf{Z} \text{ that appear in } \mathsf{E}\right\}$$

For instance:

$$\left|\mathsf{X}^{(1,0,1,0)}\mathsf{Z}^{(0,0,1,1)}\right| = |\mathsf{X} \otimes \mathsf{I} \otimes \mathsf{XZ} \otimes \mathsf{Z}| = |\mathsf{X} \otimes \mathsf{I} \otimes (-i\mathsf{Y}) \otimes \mathsf{Z}| = 3$$

Admissible subgroup minimum distance:

Given an admissible subgroup $\mathbb{S}$ of $\mathbb{G}_n$, we define its minimum distance as,

$$d \stackrel{\text{def}}{=} \min\left(|\mathsf{E}| : \ \mathsf{E} \text{ error of type } \mathsf{B}\right) = \min\left(|\mathsf{E}| : \ \mathsf{E} \notin \mathbb{S}\right)$$

Exercise:

What is the minimum distance of $\text{Vect}(|000\rangle, |111\rangle)$? Don't forget to exhibit the associated admissible subgroup

Theorem:

$\mathcal{C}$ stabilizer code of minimum distance d, and $|\psi\rangle \in \mathcal{C}$ be corrupted by an error $\mathsf{E} \in \mathbb{G}_n$ of weight $t < d/2$, then $|\psi\rangle$ can be recovered

Proof:

1. $\mathsf{E}\,|\psi\rangle \xrightarrow{\textit{measurement}} \mathsf{E}\,|\psi\rangle$ giving the classical information $\sigma(\mathsf{E})$
2. Find classically minimum weight $\mathsf{E}' \in \mathbb{G}_n$ such that $\sigma(\mathsf{E}') = \sigma(\mathsf{E})$, in particular $|\mathsf{E}'| \leq |\mathsf{E}| = t$

   $\longrightarrow$ We need: efficient classical algorithm coming with the stabiliser group for this task
3. Apply E'. But why does it work?

$$\sigma(\mathsf{E}'\mathsf{E}) = \sigma(\mathsf{E}') + \sigma(\mathsf{E}) = 0 \quad \text{and} \quad |\mathsf{E}'\mathsf{E}| \leq |\mathsf{E}'| + |\mathsf{E}| \leq 2t < d$$

Therefore, by definition of the minimum distance: $\mathsf{E}'\mathsf{E} \in \mathbb{S}$ and $\mathsf{E}'\mathsf{E}\,|\psi\rangle = |\psi\rangle$

- Decoding stabilizer codes:
  - Computing the syndrome by a projective measurement : quantum step
  - Determining the most likely error: classical step
  - Inverting the error: quantum step
- Decoding with certainty up to $d/2$ where $d = \min\left(|\mathbf{E}| \ : \ \mathbf{E} \in \mathbb{G}_n \backslash \mathbb{S}\right)$ (minimum distance)

  $\longrightarrow$ Be careful: to be efficient, we need to be efficient during the classical step
- We have seen quantum codes (and their decoding algorithm):

Shor $\subsetneq$ CSS $\subsetneq$ Stabilizer

See Exercise Session:

- Shor's code (9 qubits to protect 1 qubit) is a CSS code
- Steane's code (7 qubits to protect 1 qubit) is a CSS code using Hamming codes
- There is a stabilizer code (5 qubits to protect 1 qubit) which is not CSS

If you are interested by quantum error correcting codes:

- Kitaev's toric code in the lecture notes, Section 5, by Gilles Zémor
  https://www.math.u-bordeaux.fr/~gzemor/QuantumCodes.pdf

THRESHOLD THEOREM

I cheated during all this lecture. . .

Why?

BUT. . .

I cheated during all this lecture. . .

Why?

Noisy quantum gates?

To encode qubits: use quantum gates. . .

If quantum gates are noisy, then our encodings are not valid and our analysis is false. . .

Do we conclude that quantum codes are only useful with perfect quantum gates?

$\longrightarrow$ **No!** Hopefully. . .

Threshold theorem (admitted, see Nielsen & Chuang):

A quantum circuit containing $p(n)$ gates may be simulated with probability of error at most ε using

$$O\left(\text{poly}\left(\log\left(\frac{p(n)}{\varepsilon}\right)p(n)\right)\right)$$

gates on hardware whose components fail with probability at most p, if p is below some constant threshold, $p < p_{\text{th}}$, and given reasonable assumptions about the noise in the hardware

If the error to perform each gate is a small enough constant: arbitrarily long quantum computations to arbitrarily good precision with small overhead in the number of gates

Proof strategy:

Build recursively from noisy quantum gates better $\big($and larger$\big)$ gates with the help of codes

$\longrightarrow$ The threshold p_{th} depends of the used quantum correcting codes

To take away: Scott Aaronson

" The entire content of the Threshold Theorem is that you're correcting errors faster than they're created. That's the whole point, and the whole non-trivial thing that the theorem shows. That's the problem it solves"

EXERCISE SESSION