LECTURE 7
QUANTUM ERROR CORRECTING CODES AND A LITTLE BIT OF CLASSICAL ERROR CORRECTING CODES

INF587 Quantum computer science and applications

Thomas Debris-Alazard

Inria, École Polytechnique

Presentation of quantum error correcting codes! But we will start with the classical case

Quantum error correcting code are (roughly):

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

1. Classical error correcting codes: to be protected against classical errors
2. A first quantum error correcting code: Shor's code
3. Calderbank-Shor-Steane (CSS) codes
4. Stabilizer codes
5. Threshold theorem

Building an efficient quantum computer?

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

Decoherence ($\longleftrightarrow$ quantum noise):

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

- What does the "noise" mean?
- How to be "protected" against the "noise"?

$\longrightarrow$ Do the classical computation also suffer of errors during computations?

Building an efficient quantum computer?

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

Decoherence ($\longleftrightarrow$ quantum noise):

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

- What does the "noise" mean?
- How to be "protected" against the "noise"?

$\longrightarrow$ Do the classical computation also suffer of errors during computations?

Yes!

How do we proceed to be protected against errors in classical computation?

In the early age: errors in computation, big issue!

$\longrightarrow$ Read the story of R. Hamming in the Bell labs (1947):

https://en.wikipedia.org/wiki/Romeo_Hamming

Classically:

- Resource that we need to protect: the bits 0 and 1
- Errors: bits are flipped $\begin{cases} 0 \mapsto 1 \\ 1 \mapsto 0 \end{cases}$

Breakthrough: Shannon (1948/1949) gave the foundations to protect classical computations against errors but not only!

Protection against errors in computation $\subseteq$ Information theory

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 (not only "flip"...)
- **Problem 3:** Impossibility to copy qubits before working on it (no cloning theorem)
- **Problem 4:** Measurements modify the qubits...

To overcome these issues: take a look on how we proceed in the classical case!

CLASSICAL ERROR CORRECTING CODES

THE PROBLEM

Suppose that we send bits across a noisy channel

$001011 \rightsquigarrow 001111$

How can the receiver detect that an error occurred and correct it?

Suppose that we send bits across a noisy channel

$$001011 \rightsquigarrow 001111$$

How can the receiver detect that an error occurred and correct it?

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

THE SOLUTION

An example: over the phone

M like Mike, O like Oscar, R like Romeo, A like Alpha, etc...

- We perform an **encoding** (*i.e.*, adding redundancy):

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

- We send the names across the noisy channel (given by a bad communication over the phone):

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

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

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

A naive solution: the 3-bits repetition code

Encode bits as:

$$0 \mapsto 000 \quad \text{and} \quad 1 \mapsto 111$$

Binary Symmetric Channel:

Suppose that bits are independently flipped with probability $p < 1/2$

For instance:

$000 \rightsquigarrow 010$ with probability $p(1-p)^2$, $000 \rightsquigarrow 011$ with probability $(1-p)p^2$, etc...

- Decoding: given $b_1 b_2 b_3$ choose the bit that has the majority

$$010 \mapsto 0 \quad \text{and} \quad 110 \mapsto 1$$

Does the 3-bits repetition code offer a better protection against errors than just sending the bit?

A naive solution: the 3-bits repetition code

Encode bits as:

$$0 \mapsto 000 \quad \text{and} \quad 1 \mapsto 111$$

Binary Symmetric Channel:

Suppose that bits are independently flipped with probability $p < 1/2$

For instance:

$000 \rightsquigarrow 010$ with probability $p(1-p)^2$, $000 \rightsquigarrow 011$ with probability $(1-p)p^2$, etc...

- **Decoding**: given $b_1 b_2 b_3$ choose the bit that has the majority

$$010 \mapsto 0 \quad \text{and} \quad 110 \mapsto 1$$

Does the 3-bits repetition code offer a better protection against errors than just sending the bit?

$\longrightarrow$ **Yes**! The probability that choosing the bit that has the majority is the correct choice is

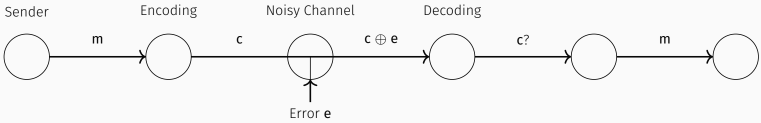
$$3(1-p)^2 p + (1-p)^3 > 1-p$$

MORE FORMALLY: LINEAR CODES

How to transmit k bits over a **noisy channel**?

1. **Linear code:** fix $\mathcal{C}$ subspace $\subseteq \mathbb{F}_2^n$ of dimension $k < n$
2. **Encoding:** map $(m_1, \ldots, m_k) \longrightarrow \mathbf{c} = (c_1, \ldots, c_n) \in \mathcal{C}$ task adding $n - k$ bits redundancy

   $\longrightarrow$ as $\mathcal{C}$ is linear the encoding is easy (only linear algebra)
3. Send $\mathbf{c}$ across the noisy channel, **bits of c are independently flipped with probability p**



Decoding:

$\longrightarrow$ from $\mathbf{c} \oplus \mathbf{e}$: recover $\mathbf{e}$ and then $\mathbf{c}$ (using the linearity, we easily recover $\mathbf{m}$ from $\mathbf{c}$)

Linear Code:

A linear code $\mathcal{C}$ of length n and dimension k ($[n,k]$-code): subspace of $\mathbb{F}_2^n$ of dimension k

Dual code:

Given $\mathcal{C}$, its dual $\mathcal{C}^\perp$ is the $[n, n-k]$-code

$$\mathcal{C}^\perp \stackrel{\text{def}}{=} \left\{ \mathbf{c}^\perp \in \mathbb{F}_2^n \;:\; \forall \mathbf{c} \in \mathcal{C},\; \langle \mathbf{c}, \mathbf{c}^\perp \rangle = \sum_{i=1}^{n} c_i c_i^\perp = 0 \in \mathbb{F}_2 \right\}.$$

Remark: $\mathcal{C}^\perp$ orthogonal group of $\mathcal{C}$ in the character theory

The repetition code:

The n-repetition code is the following $[n, 2]$-code:

$$\left\{ (\underbrace{0, \ldots, 0}_{\text{n times}}),\; (\underbrace{1, \ldots, 1}_{\text{n times}}) \right\}$$

$\longrightarrow$ Using majority voting enables to correct $< n/2$ errors!

But, huge cost of protection: n bits to protect 1 bit...

$\mathcal{C}$ is a subspace of $\mathbb{F}_2^n$ of dimension k: choose a basis $\mathbf{b}_1, \dots, \mathbf{b}_k$ to represent it!

$\longrightarrow$ Many times this representation is not the most "useful"

Parity-check matrix:

Let $\mathbf{h}_1, \cdots, \mathbf{h}_{n-k}$ be a basis of $\mathcal{C}^\perp$, then

$$\mathcal{C} = \left\{ \mathbf{c} : \mathbf{H}\mathbf{c}^{\mathsf{T}} = \mathbf{0} \right\} \quad \text{where the rows of } \mathbf{H} \in \mathbb{F}_2^{(n-k)\times n} \text{ are the } \mathbf{h}_i\text{'s}$$

The matrix $\mathbf{H}$ is called a parity-check matrix of $\mathcal{C}$.

Given two finite subspaces of $\mathbb{F}_2^n$: $F \subseteq E$.

Equivalence relation: $x \sim y \iff x - y \in F$.

$$E/F = \{\overline{x} \ : \ x \in E\} \quad \text{where } \overline{x} \stackrel{\text{def}}{=} \{y \in E \ : \ x \sim y\} = x + F$$

$\longrightarrow$ It defines a linear space!

$$k = \mathbf{dim}\, E/F = \mathbf{dim}\, E - \mathbf{dim}\, F, \text{ in particular: } \sharp E/F = 2^k$$

Rough analogy:

E/F	$\mathbb{Z}/4\mathbb{Z}$
$\{\overline{x_1}, \ldots, \overline{x_{2^k}}\}$	$\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$
$\overline{x_i} = x_i + F$	$\overline{\ell} = \ell + 4\mathbb{Z}$
$\overline{x} = \overline{y} \iff x - y \in F$	$\overline{\ell} = \overline{m} \iff \ell - m \in 4\mathbb{Z}$
$E = \bigsqcup_{1 \leq i \leq 2^k} \overline{x_i}$	$\mathbb{Z} = \bigsqcup_{\ell \in \{0,1,2,3\}} \overline{\ell}$

Decoding: given $\mathbf{c} \oplus \mathbf{e}$, recover $\mathbf{e}$.

$\longrightarrow$ Make modulo $\mathcal{C}$ to extract the information about $\mathbf{e}$

Coset space: $\mathbb{F}_2^n/\mathcal{C}$

$$\sharp\, \mathbb{F}_2^n/\mathcal{C} = 2^{n-k} \quad \text{and} \quad \mathbb{F}_2^n/\mathcal{C} = \left\{ \overline{\mathbf{x}}_i \ : 1 \leq i \leq 2^{n-k} \right\} = \left\{ \mathbf{x}_i + \mathcal{C} \ : \ 1 \leq i \leq 2^{n-k} \right\}$$

where the $\mathbf{x}_i$'s are the representatives of $\mathbb{F}_2^n/\mathcal{C}$. The $x_i + \mathcal{C}$'s are disjoint!

A natural set of representatives via a parity-check $\mathbf{H}$: syndromes

$$\mathbf{x}_i + \mathcal{C} \in \mathbb{F}_q^n/\mathcal{C} \longmapsto \mathbf{H}\mathbf{x}_i^{\intercal} \in \mathbb{F}_2^{n-k} \text{ (called a syndrome)}$$

is an isomorphism

$$\mathbb{F}_2^n = \bigsqcup_{\mathbf{s} \in \mathbb{F}_2^{n-k}} \left\{ \mathbf{z} \in \mathbb{F}_2^n \ : \ \mathbf{H}\mathbf{z}^{\intercal} = \mathbf{s}^{\intercal} \right\}$$

$$\mathbf{c} \oplus \mathbf{e} \bmod \mathcal{C} = \mathbf{H}(\mathbf{c} \oplus \mathbf{e})^{\intercal} = \underbrace{\mathbf{H}\mathbf{c}^{\intercal}}_{=0} \oplus \mathbf{H}\mathbf{e}^{\intercal} = \mathbf{H}\mathbf{e}^{\intercal} \text{ which gives information to recover } \mathbf{e} \text{ (decoding)}$$

$\longrightarrow$ $\mathbf{H}\mathbf{e}^{\intercal}$ is only function of $\mathbf{e}$!

Let $\mathcal{C}_{\text{Ham}}$ be the $[7,4]$-code of parity-check matrix:

$$\mathbf{H} \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Let $\mathbf{c} \oplus \mathbf{e}$ where $\begin{cases} \mathbf{c} \in \mathcal{C}_{\text{Ham}} \\ \text{only one bit of } \mathbf{e} \text{ is } 1 \end{cases}$: how to easily recover $\mathbf{e}$?

Let $\mathcal{C}_{\mathrm{Ham}}$ be the $[7,4]$-code of parity-check matrix:

$$\mathbf{H} \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Let $\mathbf{c} \oplus \mathbf{e}$ where $\begin{cases} \mathbf{c} \in \mathcal{C}_{\mathrm{Ham}} \\ \text{only one bit of } \mathbf{e} \text{ is } 1 \end{cases}$: how to easily recover $\mathbf{e}$?

1. Compute the associated syndrome:
$$\mathbf{H}(\mathbf{c} \oplus \mathbf{e})^{\mathsf{T}} = \mathbf{H}\mathbf{c}^{\mathsf{T}} \oplus \mathbf{H}\mathbf{e}^{\mathsf{T}} = \mathbf{H}\mathbf{e}^{\mathsf{T}}$$
2. $\mathbf{e}$ has only one non-zero bit, $\mathbf{H}\mathbf{e}^{\mathsf{T}}$ is a column of $\mathbf{H}$
3. Columns of $\mathbf{H}$ are the binary representation of $1, 2, \cdots, 7$: $\mathbf{H}\mathbf{e}^{\mathsf{T}}$ gives (in binary) the position where there is an error!

Hamming codes can correct one error!

$\longrightarrow$ There are more clever codes than repetition or Hamming codes... In particular these codes don't seem "good". We will see later a criteria (minimum distance) for "good codes"

- Nice lecture notes by Alain Couvreur (with a focus on algebra):
  `http://www.lix.polytechnique.fr/~alain.couvreur/doc_ens/lecture_notes.pdf`
- The "bible" of error correcting codes: "*The theory of error correcting codes*", F.J. MacWilliams , N.J.A. Sloane (1978)

Error correcting codes have a huge impact in theoretical computer science, cryptography, communications, quantum key distribution (QKD), etc...

$\longrightarrow$ Let's go back to the quantum case!

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?

BE INSPIRED BY THE CLASSICAL CASE

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?

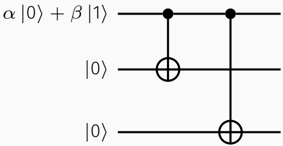
No! No-cloning theorem...

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:



Inspired by the classical case: flip the qubits: 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: 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?

$\longrightarrow$ Use a parity-check matrix!

$\mathbf{H} \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ 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 $|\mathbf{x}\rangle \otimes |00\rangle \mapsto |\mathbf{x}\rangle \otimes \left|\mathbf{x}\mathbf{H}^{\mathsf{T}}\right\rangle$ 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 $(\mathbf{X}^2 = \mathbf{I}_2)$

$\longrightarrow$ 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

Fundamental idea (I): decompose the three qubit 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

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

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

Fundamental idea (I): decompose the three qubit 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

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

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

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

Fundamental idea (II): syndrome measurement

Measure according to (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?

Fundamental idea (I): decompose the three qubit 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

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

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

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

Fundamental idea (II): syndrome measurement

Measure according to (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

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

- With probability one we measure 2 (“we are in $\mathcal{C}_2$”) 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 "no error": do nothing,
- With probability $|b|^2$ observe "error on the first qubit", the quantum state collapses to

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

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

OTHER KIND OF ERRORS?

What is the most important sentence of INF587*?*

OTHER KIND OF ERRORS?

What is the most important sentence of INF587*?*

$\longrightarrow$ 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 error 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 $\mathsf{Z} \equiv$ 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 $\alpha|000\rangle + \beta|111\rangle$:

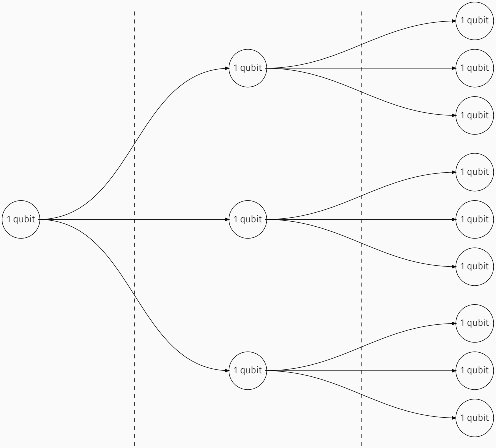
$$\alpha|+++\rangle + \beta|---\rangle$$

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

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

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

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

Encoding

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

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

$\longrightarrow$ The encoding belongs to the linear code of dimension 3 generated by

(111000000), (000111000), (000000111)

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

$$\mathcal{C}_0 \stackrel{\text{def}}{=} \text{Vect}\left(|111000000\rangle, |000111000\rangle, |000000111\rangle\right),$$

$$\mathcal{C}_1 \stackrel{\text{def}}{=} \text{Vect}\left(|011000000\rangle, |100111000\rangle, |100000111\rangle\right), \quad \text{etc...}$$

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

Z-error on either 1st, 2nd or 3rd (*resp.* 4th, 5th or 6th) qubit yields:

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

- 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:

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

Decoding

Measure (it does not change the quantum state) 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 $\mathbf{X}$ and one error of type $\mathbf{Z}$!

Exercise

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

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

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

But there is a moral

Errors on qubits: apply Pauli matrices

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

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

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

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

Exercise Session 2

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 $\mathbf{M}$ 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 $\mathbf{X}$, $\mathbf{Z}$ and $\mathbf{XZ}$

Correcting a discrete set of errors by syndrome measurement: $\mathbf{X}$ and $\mathbf{Z}$
$\longrightarrow$ We can automatically correct a much larger (continuous!) class of errors.

Intuitively: if syndrome measurement correct with certainty, performing this measurement after applying $\mathbf{U}$ will collapse the quantum state into no error, error of type-$\mathbf{X}$ and $\mathbf{Z}$

Shor's code can correct all errors of type $\mathbf{X}$ and $\mathbf{Z}$!

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 (continuous) error provided they only affect a single qubit

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

Is it useful, namely better than doing nothing?

$\longrightarrow$ Yes! See Lecture 8 for a rigorous proof of this statement

(for the depolarizing channel)

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

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

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 $\mathcal{C}$, and using the notation

$$|\mathcal{C}\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{\sharp\mathcal{C}}} \sum_{\mathbf{c}\in\mathcal{C}} |\mathbf{c}\rangle$$

we have

$$\mathsf{H}^{\otimes n} |\mathcal{C}\rangle = \left|\mathcal{C}^{\perp}\right\rangle$$

Proof

See exercise session

But from which result this lemma comes from?

Lemma

For any linear code $\mathcal{C}$, and using the notation

$$|\mathcal{C}\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{\sharp\mathcal{C}}} \sum_{\mathbf{c}\in\mathcal{C}} |\mathbf{c}\rangle$$

we have

$$\mathsf{H}^{\otimes n} |\mathcal{C}\rangle = \left|\mathcal{C}^{\perp}\right\rangle$$

Proof

See exercise session

But from which result this lemma comes from?

$\longrightarrow$ Poisson summation formula (Exercise Session 5)

- defined from two linear codes $(\mathcal{C}_X, \mathcal{C}_Z)$ of length n such that $\mathcal{C}_Z \subseteq \mathcal{C}_X$

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

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

There are efficient one-to-one mappings (see exercise session)

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

CSS quantum codes

CSS codes encodes k qubits as

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

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

Exercise session

How to efficiently build CSS encodings?

$\longrightarrow$ As for Shor's code, use: syndrome measurement

Syndrome measurement

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

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

$\longrightarrow$ 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 $\mathbf{H}\mathbf{e}^{\mathsf{T}} = \mathbf{s}^{\mathsf{T}}$.

$\longrightarrow$ 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:

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

(because: $\forall x \in \mathcal{C}_X, c_Z \in \mathcal{C}_Z, H_X(x + c_Z)^\top = 0$ as $x, c_Z \in \mathcal{C}_X$)

Syndrome measurement

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

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

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

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

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

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

ABILITY TO CORRECT CLASSICAL ERRORS?

Up to now we used the fact that we can "decode" $\mathcal{C}_{\mathsf{X}}$ and $\mathcal{C}_{\mathsf{Z}}^{\perp}$

Let, $\mathbf{H}_{\mathsf{X}}$ and $\mathbf{H}_{\mathsf{Z}}$ be a parity-check matrix of $\mathcal{C}_{\mathsf{X}}$ and $\mathcal{C}_{\mathsf{Z}}^{\perp}$

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

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

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

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

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 $\mathcal{C} \subseteq \mathbb{F}_2^n$, 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 proof in 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 $n/2$ (see exercise session)

- 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 (hopefully for telecommunication) but to understand how deserves a full course

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 (even $\ll d/2$)

$\longrightarrow$ Active research topic with a lot a consequences, event recent (for instance the 5G...)

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

Theorem: decoding CSS codes

Let $\mathcal{C}_X$ and $\mathcal{C}_Z$ be linear codes such that $\mathcal{C}_Z \subseteq \mathcal{C}_X$

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

In particular, we can hope to decode up to $d_{\min}(\mathcal{C}_X)/2$ errors-X and $d_{\min}(\mathcal{C}_Z^{\perp})/2$ 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 $X^{\mathbf{e}}Z^{\mathbf{f}}$ or $iX^{\mathbf{e}}Z^{\mathbf{f}}$, where $\mathbf{e}, \mathbf{f} \in \mathbb{F}_2^n$, forms a multiplicative group.

Admissible subgroup

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

$\longrightarrow$ We will only consider admissible subgroups!

Lemma

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

Proof

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

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

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

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

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

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

Stabilizer code

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

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

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

An example

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

$$\{\mathsf{I} \otimes \mathsf{I} \otimes \mathsf{I}, \ \mathsf{Z} \otimes \mathsf{Z} \otimes \mathsf{I}, \mathsf{Z} \otimes \mathsf{I} \otimes \mathsf{Z}, \mathsf{I} \otimes \mathsf{Z} \otimes \mathsf{Z}\}$$

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

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

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

Notation

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

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

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

Proposition (admitted)

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

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

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

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

The syndrome function

$$\begin{array}{rcl} \sigma : \mathbb{G}_n & \longrightarrow & \{0,1\}^r \\ \mathbf{E} & \longmapsto & \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_r \end{pmatrix} \quad \text{with } s_i \stackrel{\text{def}}{=} \begin{cases} 0 & \text{if } \mathbf{E}\mathbf{M}_i = \mathbf{M}_i\mathbf{E} \\ 1 & \text{if } \mathbf{E}\mathbf{M}_i = -\mathbf{M}_i\mathbf{E} \end{cases} \end{array}$$

Remark

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

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

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

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

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

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

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

Proposition (admitted)

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

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

Linear codes	Stabilizer codes
k bits encoded in n bits	k qubits encoded in n qubits
subspace of dimension k	subspace of dimension 2^k
parity-check matrix $\mathbf{H}$	minimal generators set of $\mathbb{S}$
$r = n - k$ rows, n columns	$r = n - k$ generators
syndrome $\in \{0,1\}^{n-k}$	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: $|\psi\rangle \rightsquigarrow \mathsf{E}\,|\psi\rangle \in \mathcal{C}(\mathbf{0}) = \mathcal{C} \xrightarrow{\textit{measurement}}$ syndrome **0**, no error...

Is it a problem? It depends of **E**...

We can distinguish two types of error E with syndrome 0

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

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

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

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

$\longrightarrow$ Type **B** errors: cannot be detected and thus cannot be corrected...

To overcome this issue: introduce the minimum distance

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

$$\textit{Weight}: \quad |\mathsf{E}| \stackrel{\text{def}}{=} \sharp\{i : e_i \neq f_i \text{ or } e_i = f_i = 1\} = \sharp\{\mathsf{X}, \mathsf{Y}, \mathsf{Z} \text{ that appears in } \mathsf{E}\}$$

For instance:

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

Minimum distance

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

Exercise

What is the minimum distance of $\mathrm{Vect}(|000\rangle, |111\rangle)$?

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. $\mathsf{E}\,|\psi\rangle \xrightarrow{\text{measurement}} \mathsf{E}\,|\psi\rangle$ 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?

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

   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 $d = \mathbf{min}\left(|\mathbf{E}| \ : \ \mathbf{E} \in \mathbb{G}_n \backslash \mathbb{S}\right)$ (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.

THRESHOLD THEOREM

BUT...

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: 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 (and larger) gates with the help of codes

$\longrightarrow$ The threshold 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