Quantum error correcting codes

March 4

Plan

- 1. Introduction
- 2. The Shor code
- 3. CSS codes
- 4. Stabilizer codes
- 5. More general error models

1.Introduction

Constructing a quantum computer

$\Rightarrow$

error protection mechanism : impossibility to be completely isolated from the environment : decoherence

Very tough issue?

- **Problem 1:** Not enough to protect $|0\rangle$ and $|1\rangle$, every linear combination $\alpha |0\rangle + \beta |1\rangle$ must be protected as well
- **Problem 2 :** Much richer error model than for classical bits
- **Problem 3 :** Impossibility result ("no cloning theorem")
- **Problem 4 :** Measure modifies the qubit !

2. A first example : the Shor code

Error model

Much richer error model than for bits

- qubit inversion(X)

$$|0\rangle \rightarrow |1\rangle$$
$$|1\rangle \rightarrow |0\rangle$$

- phase error (Z)

$$|0\rangle \rightarrow |0\rangle$$
$$|1\rangle \rightarrow -|1\rangle$$

- both! (Y)

$$|0\rangle \rightarrow -i|1\rangle$$
$$|1\rangle \rightarrow i|0\rangle$$

The Pauli group

single qubit Pauli group $\mathcal{G}_1$:

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

Pauli group over n qubits $\mathcal{G}_n$: $\mathcal{G}_1 \otimes \mathcal{G}_1 \cdots \otimes \mathcal{G}_1$

$$\mathcal{G}_n \equiv \{I, X, Y, Z\}^n \times \{\pm 1, \pm i\}$$

Two error models

- Depolarizing channel : each qubit undergoes an error X, Y, Z with probability $\frac{p}{3}$, and is not modified with probability $1 - p$.
- Quantum erasure channel : each qubit is erased with probability p (and it is known if the qubit has been erased or not). when the qubit is not erased, it is not affected by any noise. If erased, the qubit undergoes a transformation I, X, Y, Z with probability $\frac{1}{4}$ for each of them

A code correcting one qubit inversion

$$|0\rangle \rightarrow |000\rangle$$
$$|1\rangle \rightarrow |111\rangle$$

This is NOT the repetition code !

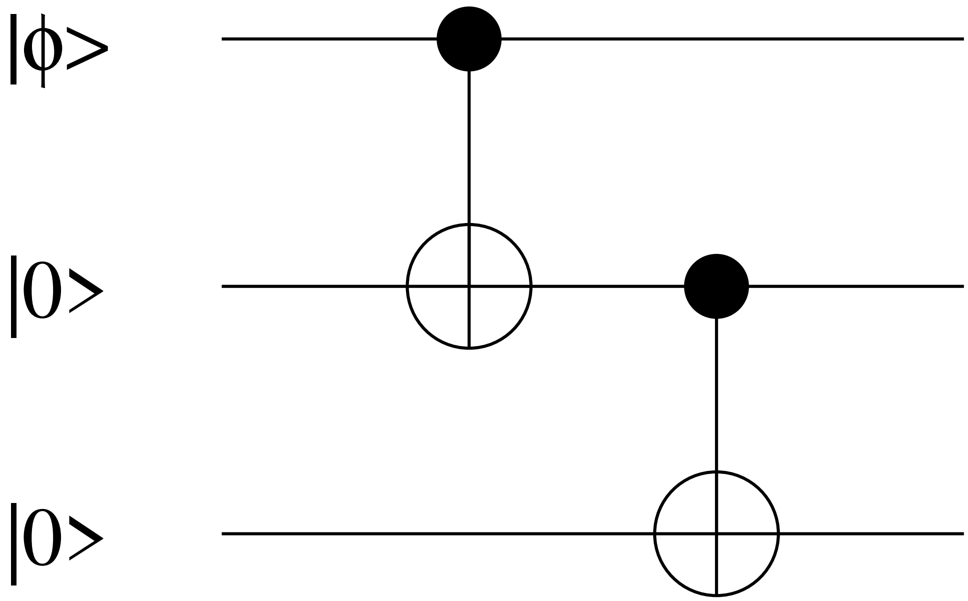
$$\alpha |0\rangle + \beta |1\rangle \rightarrow \alpha |000\rangle + \beta |111\rangle$$
$$\neq$$
$$(\alpha |0\rangle + \beta |1\rangle)^{\otimes 3}$$

Exercise

Give a circuit that realizes the encoding, i.e. a circuit performing the unitary transformation

$$|0\rangle\,|00\rangle \quad \mapsto \quad |000\rangle$$
$$|1\rangle\,|00\rangle \quad \mapsto \quad |111\rangle$$

Solution



An example

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

$\rightsquigarrow$ error X on the 2-th qubit

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

Idea

Measure without destroying the state, for $|x, y, z\rangle$ "observe" $y \oplus z, x \oplus z$:

$$\Longleftrightarrow$$

measure according to $C \oplus C_1 \oplus C_2 \oplus C_3$.

$$\text{Code} = \text{Vect}(|000\rangle, |111\rangle)$$

$$C_1 = \text{Vect}(|100\rangle, |011\rangle) \; C_2 = \text{Vect}(|010\rangle, |101\rangle) \; C_3 = \text{Vect}(|001\rangle, |110\rangle)$$

Example : error on the 2-th qubit

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

$\downarrow$ measure : "we are in C_2"

$\alpha\,|010\rangle + \beta\,|101\rangle$ N.B. same state!

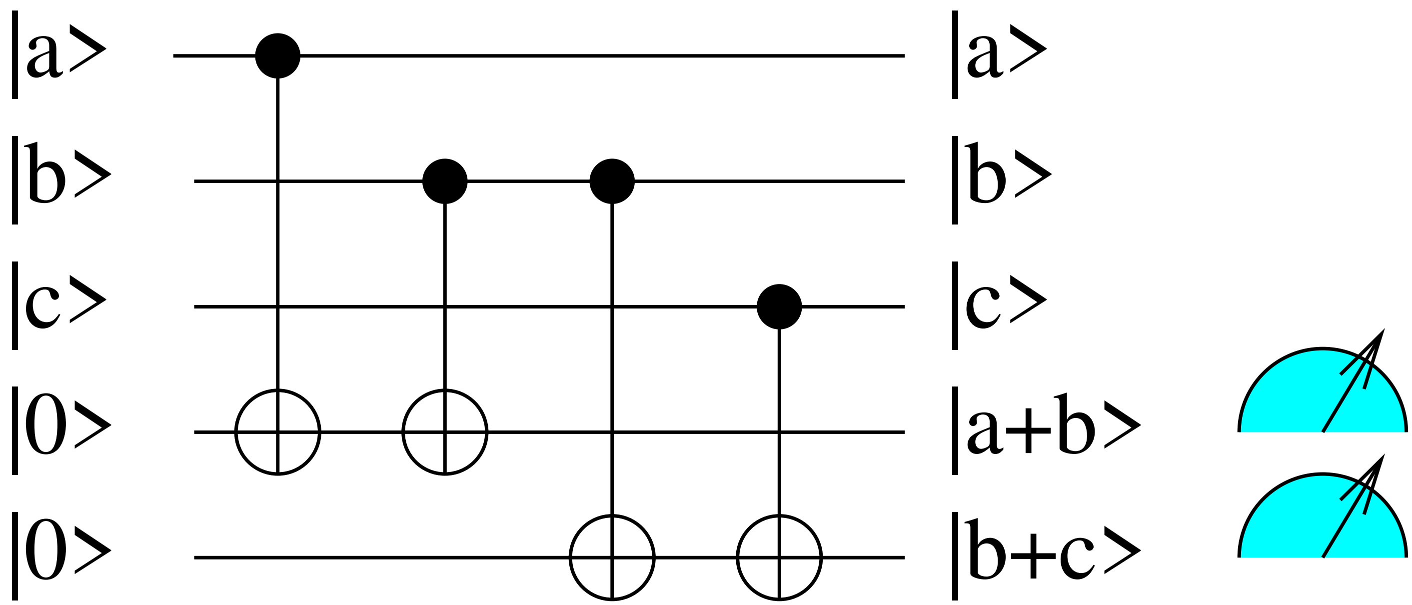
$\downarrow$ inverting 2-th qubit

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

Exercise

Give a circuit that performs the decoding

Solution



More general errors can also be corrected:

$$|000\rangle \rightsquigarrow a\,|000\rangle + b\,|100\rangle + c\,|010\rangle + d\,|001\rangle$$

Same decoding algorithm : measure according to $C \oplus C_1 \oplus C_2 \oplus C_3$:

- with prob. $|a|^2$ observe "no error" and get $|000\rangle$,
- with prob. $|b|^2$ observe "error on the first qubit", after measuring we get $|100\rangle$ and invert the first qubit.

This code is useless against Z errors :

$$\alpha\,|000\rangle + \beta\,|111\rangle \rightsquigarrow \alpha\,|000\rangle - \beta\,|111\rangle \in C$$

error of type Z = error of type X in the basis

$$|\psi_0\rangle \stackrel{\text{def}}{=} \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|\psi_1\rangle \stackrel{\text{def}}{=} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

In this base the error acts as :

$$\begin{aligned} |\psi_0\rangle &\rightsquigarrow |\psi_1\rangle \\ |\psi_1\rangle &\rightsquigarrow |\psi_0\rangle \end{aligned}$$

This gives the following encoding :

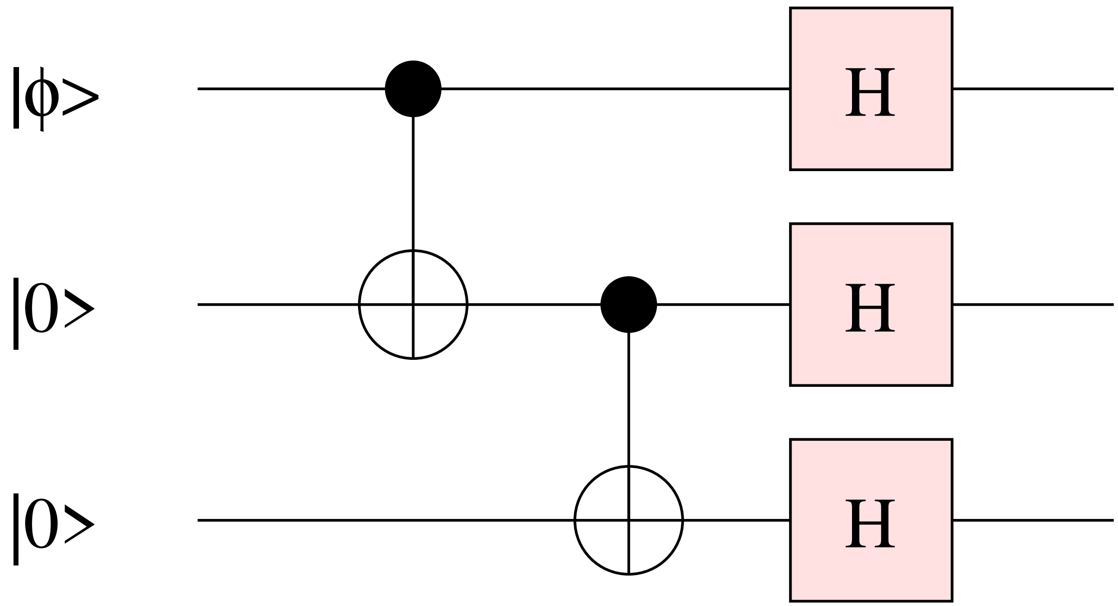
$$\alpha |0\rangle + \beta |1\rangle \to \alpha |\psi_0\rangle |\psi_0\rangle |\psi_0\rangle + \beta |\psi_1\rangle |\psi_1\rangle |\psi_1\rangle .$$

Exercise

Give the corresponding encoding circuit, i.e. a circuit that corresponds to the unitary transform U such that

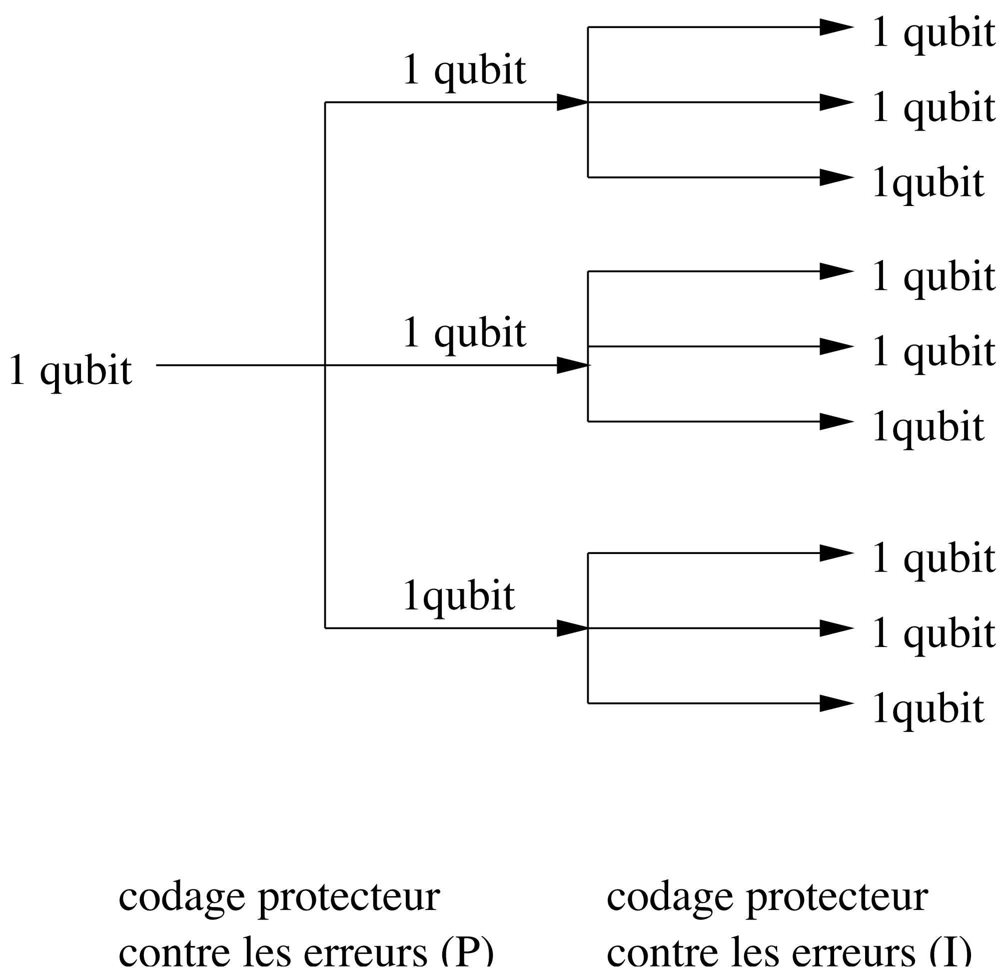
$$\begin{aligned} |0\rangle\,|00\rangle &\mapsto |\psi_0\rangle\,|\psi_0\rangle\,|\psi_0\rangle \\ |1\rangle\,|00\rangle &\mapsto |\psi_1\rangle\,|\psi_1\rangle\,|\psi_1\rangle \end{aligned}$$

Solution



Correcting both types of error

Concatenation



Encoding

$$
\begin{aligned}
|0\rangle \rightarrow (|0\rangle + |1\rangle)^{\otimes 3} \quad &\rightarrow \quad (|000\rangle + |111\rangle)^{\otimes 3} \\
|1\rangle \rightarrow (|0\rangle - |1\rangle)^{\otimes 3} \quad &\rightarrow \quad (|000\rangle - |111\rangle)^{\otimes 3}
\end{aligned}
$$

Decoding

$$(|010\rangle + |101\rangle)(|100\rangle - |011\rangle)(|000\rangle + |111\rangle)$$

$\downarrow$ correct the (X) errors

$$(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)$$

$\downarrow$ correct the (Z) errors

$$(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

Exercise

1. Show that the Shor code corrects all X, Y and Z errors on one qubit
2. Find an error on 2 qubits which can not be corrected by Shor's code

Solution

1. done in one step for X and Z errors, Y errors are corrected in two steps since $Y = iXZ$
2. two X errors on the same block

3. The CSS codes

3. The CSS codes

- CSS = Calderbank-Shor-Steane codes
- A construction of quantum codes from classical codes
- Shor's code is a CSS code
- Construction based on two classical codes: the first one corrects X errors, the other Z errors

Classical linear code

Definition 1. [binary linear code] *A binary linear code $\mathcal{C}$ is a subspace of $\mathbb{F}_2^n$*

Can be specified by a basis

$$\mathcal{C} = \text{Vect}\{\mathbf{c}_1, \ldots, \mathbf{c}_k\}$$

Definition 2. [length and dimension] *n is the length of $\mathcal{C}$ and k the dimension of $\mathcal{C}$ as a subspace of $\mathbb{F}_2^n$ is the dimension of the code*

Definition 3. [Generator matrix] *The generator matrix of a code $\mathcal{C}$ is a matrix $\mathbf{G}$ whose rows span the code*

$$\mathcal{C} = \{\mathbf{x}\mathbf{G} | \mathbf{x} \in \mathbb{F}_2^k\}.$$

Parity-check matrix and dual code

Definition 4. [dual code] *The dual code* $\mathcal{C}^{\perp}$ *of a linear code* $\mathcal{C} \subset \mathbb{F}_2^n$ *is defined by*

$$\mathcal{C}^{\perp} \stackrel{\text{def}}{=} \{\mathbf{x} \in \mathbb{F}_2^n : \mathbf{x} \cdot \mathbf{c} = 0,\ \forall \mathbf{c} \in \mathbb{C}\}$$

Definition 5. [parity-check matrix] *The parity-check matrix of a linear code* $\mathcal{C}$ *of dimension* k *and length* n *is an* $(n-k) \times n$ *matrix* $\mathbf{H}$ *whose kernel is the code:*

$$\mathcal{C} = \{\mathbf{x} \in \mathbb{F}_2^n | \mathbf{H}\mathbf{x}^t = 0\}.$$

Minimum distance

Definition 6. [minimum distance] *The minimum distance* d

$$d \stackrel{\text{def}}{=} \min\{d_H(x,y); x \neq y \in code\}$$

d_H *: Hamming distance*

Fact 1.

$$d = \min\{w_H(x), x \neq 0 \in code\}$$

w_H *: Hamming weight*

error correction capacity : $\stackrel{\text{def}}{=} \lfloor \frac{d-1}{2} \rfloor$ = maximum number of errors that are always corrected by a decoder which outputs the closest codeword

Exercise: proving that there are codes with large minimum distance

We assume here that a binary code $\mathcal{C}$ of length n is drawn at random by choosing an $(n-k) \times n$ parity-check matrix for it uniformly at random.

1. Let $\mathbf{x} \in \mathbb{F}_2^n \setminus \{0\}$. Compute $\mathbf{Prob}(x \in \mathcal{C})$
2. Compute $\mathbb{E}(n_t)$ where $n_t \stackrel{\text{def}}{=}$ number of codewords in $\mathcal{C}$ of weight t
3. What is $\mathbb{E}(n_{\leq t})$ where $n_{\leq t} \stackrel{\text{def}}{=}$ number of non-zero codewords of weight $\leq t$?
4. What can you say when $\mathbb{E}(n_{\leq t}) < 1$?
5. Let $h(x) \stackrel{\text{def}}{=} -x \log_2(x) - (1-x)\log_2(1-x)$. By using $\sum_{i=1}^{t-1} \binom{n}{i} \leq 2^{nh(t/n)}$ which holds whenever $t/n \leq 1/2$ prove that there exists a code of minimum distance $\geq t$ and dimension $\geq k$ as soon as

$$1 - h(t/n) > k/n$$

Solution

1. $\mathbf{Prob}(\mathbf{x} \in \mathcal{C}) = \frac{1}{2^{n-k}}$

2.

$$\begin{aligned} n_t &= \sum_{x:|x|=t} 1_{x\in\mathcal{C}} \\ \Rightarrow \mathbb{E}(n_t) &= \sum_{x:|x|=t} \mathbb{E}\left(1_{x\in\mathcal{C}}\right) \\ &= \sum_{x:|x|=t} \mathbf{Prob}(x \in \mathcal{C}) \\ &= \frac{\binom{n}{t}}{2^{n-k}} \end{aligned}$$

3.

$$
\begin{aligned}
n_{\leq t} &= \sum_{s=1}^{t} n_s \\
\Rightarrow \mathbb{E}(n_{\leq t}) &= \sum_{s=1}^{t} \mathbb{E}(n_s) \\
&= \frac{\sum_{s=1}^{t} \binom{n}{s}}{2^{n-k}}
\end{aligned}
$$

4. When $\mathbb{E}(n_{\leq t}) < 1$ there exists a code in this family of minimum distance $\geq t+1$

5. Since $\mathbb{E}\left(n_{\leq t-1}\right) \leq 2^{nh(t/n)+k-n} < 1$ if $1 - h(t/n) > k/n$ we have the desired result (and the code is necessarily of dimension $\geq k$).

CSS Construction

- defined from two binary linear codes $\mathcal{C}_X$ and $\mathcal{C}_Z$ satisfying

$$\boxed{\mathcal{C}_Z^{\perp} \subset \mathcal{C}_X}$$

Definition 7. [CSS code] *The CSS code associated to the pair* $(\mathcal{C}_X, \mathcal{C}_Z)$ *is the quantum code generated by the basis*

$$|\bar{w}\rangle = \frac{1}{\sqrt{2^{k_Z^{\perp}}}} \sum_{v \in C_Z^{\perp}} |v + w\rangle$$

where w *is a set of representatives of the* 2^k *cosets of* $\mathcal{C}_Z^{\perp}$ *in* $\mathcal{C}_X$ *where*

$$k \stackrel{\text{def}}{=} \dim(C_X) - \underbrace{C_Z^{\perp}}_{k_Z^{\perp}}$$

Exercise : the Shor code

Show that the following codes are CSS codes and give $(\mathcal{C}_X, \mathcal{C}_Z)$ for them

1. $\mathbf{Vect}\left\{|000\rangle, |111\rangle\right\}$
2. $\mathbf{Vect}\left\{(|0\rangle + |1\rangle)^{\otimes 3}, (|0\rangle - |1\rangle)^{\otimes 3}\right\}$
3. the Shor code $\mathbf{Vect}\left\{(|000\rangle + |111\rangle)^{\otimes 3}, (|000\rangle - |111\rangle)^{\otimes 3}\right\}$

Solution

1.

$$
\begin{aligned}
\mathcal{C}_Z^{\perp} &= \{000\} \\
\mathcal{C}_Z &= \{0,1\}^3 \\
\mathbf{G}_X &= \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}
\end{aligned}
$$

2.

$$
\begin{aligned}
\mathcal{C} &= \mathbf{Vect}\left\{ \sum_{x:|x| \text{ even}} |x\rangle + \sum_{x:|x| \text{ odd}} |x\rangle \, , \sum_{x:|x| \text{ even}} |x\rangle - \sum_{x:|x| \text{ odd}} |x\rangle \right\} \\
&= \mathbf{Vect}\left\{ \sum_{x:|x| \text{ even}} |x\rangle \, , \sum_{x:|x| \text{ odd}} |x\rangle \right\} \\
\mathcal{C}_Z^{\perp} &= \{000, 011, 101, 110\}, \quad \mathbf{G}_Z = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \\
\mathcal{C}_X &= \{0,1\}^3
\end{aligned}
$$

3.

$$\mathbf{G}_X = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$\mathbf{H}_Z = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$\mathbf{G}_Z = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Exercise: the Steane code

Let $\mathcal{C}_X = \mathcal{C}_Z$ be given by the following parity matrix

$$\mathbf{H} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

1. Prove that $\mathbf{H}\mathbf{H}^{\mathsf{T}} = 0$
2. Prove that $\mathcal{C}_Z^{\perp} \subset \mathcal{C}_X$
3. Give a description of the CSS code associated to $(\mathcal{C}_X, \mathcal{C}_Z)$

Solution

1. obvious
2. obvious
3. C_X and C_Z have as generator matrix

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

The first row of $\mathbf{G}$ and the all 1 vector $\mathbf{1}$ does not belong to $C_Z^{\perp}$. The code is generated by the two states

$$|\bar{0}\rangle = \sum_{v \in \mathcal{C}_Z^{\perp}} |v\rangle$$

$$|\bar{1}\rangle = \sum_{v \in \mathcal{C}_Z^{\perp}} |\mathbf{1} + v\rangle$$

Action of t X errors on a CSS code

$\mathbf{e} \in \{0,1\}^n$ s.t. $|\mathbf{e}| = t$ and

$$\frac{1}{\sqrt{2^{k_Z^\perp}}} \sum_{\mathbf{v} \in C_Z^\perp} |\mathbf{v} + \mathbf{w}\rangle \rightsquigarrow \frac{1}{\sqrt{2^{k_Z^\perp}}} \sum_{\mathbf{v} \in C_Z^\perp} |\mathbf{v} + \mathbf{w} + \mathbf{e}\rangle$$

- The affine spaces $\mathbf{x} + \mathcal{C}_X$ in $\{0,1\}^n$ are disjoint $\Rightarrow$ the spaces $\mathbf{Vect}\left\{|\mathbf{x} + \mathbf{c}_X\rangle, \mathbf{c}_X \in \mathcal{C}_X\right\}$ define a projective measurement
- We recover $\mathbf{e}$ if $2t + 1 \leq d_X$, $d_X \stackrel{\text{def}}{=}$ minimum distance of C_X.
- Action of C_X : correct X errors

Action of t Z errors on a CSS code

$\mathbf{e} \in \{0,1\}^n$ s.t. $|e| = t$ representing phase errors

$$\frac{1}{\sqrt{2^{k_Z^\perp}}} \sum_{\mathbf{v} \in C_Z^\perp} |\mathbf{v} + \mathbf{w}\rangle \rightsquigarrow \frac{1}{\sqrt{2^{k_Z^\perp}}} \sum_{\mathbf{v} \in C_Z^\perp} (-1)^{(\mathbf{v}+\mathbf{w}).\mathbf{e}} |\mathbf{v} + \mathbf{w}\rangle$$

Idea : correct phase errors by correcting X errors in the Hadamard basis

Reminder :

$$H^{\otimes n} : |x\rangle \to \frac{1}{\sqrt{2^n}} \sum_y (-1)^{x.y} |y\rangle$$

Correcting phase errors

$$\frac{1}{\sqrt{2^{k_Z^\perp}}} \sum_{\mathbf{v} \in C_Z^\perp} (-1)^{(\mathbf{v}+\mathbf{w}).\mathbf{e}} |\mathbf{v}+\mathbf{w}\rangle \overset{H^{\otimes n}}{\mapsto} \frac{1}{\sqrt{2^{k_Z^\perp + n}}} \sum_{\substack{\mathbf{x} \in \{0,1\}^n \\ \mathbf{v} \in C_Z^\perp}} (-1)^{(\mathbf{v}+\mathbf{w}).(\mathbf{e}+\mathbf{x})} |\mathbf{x}\rangle$$

Note that

$$\begin{aligned}
\sum_{\substack{\mathbf{x} \in \{0,1\}^n \\ \mathbf{v} \in C_Z^\perp}} (-1)^{(\mathbf{v}+\mathbf{w}).(\mathbf{e}+\mathbf{x})} |\mathbf{x}\rangle &= \sum_{\substack{\mathbf{y} \in \{0,1\}^n \\ \mathbf{v} \in C_Z^\perp}} (-1)^{(\mathbf{v}+\mathbf{w}).\mathbf{y}} |\mathbf{y}+\mathbf{e}\rangle \\
&= \sum_{\mathbf{y}} (-1)^{\mathbf{w}.\mathbf{y}} \sum_{\mathbf{v} \in C_Z^\perp} (-1)^{\mathbf{v}.\mathbf{y}} |\mathbf{y}+\mathbf{e}\rangle
\end{aligned}$$

Correcting phase errors(II)

Since $\sum_{\mathbf{v}\in C_Z^\perp}(-1)^{\mathbf{v}.\mathbf{y}} = |C_Z^\perp|$ if $\mathbf{y} \in C_Z$ and 0 else, we obtain

$$\sum_{\substack{\mathbf{x}\in\{0,1\}^n \\ \mathbf{v}\in C_Z^\perp}} (-1)^{(\mathbf{v}+\mathbf{w}).(\mathbf{e}+\mathbf{x})} |\mathbf{x}\rangle = |C_Z^\perp| \sum_{\mathbf{y}\in C_Z} (-1)^{\mathbf{w}.\mathbf{y}} |\mathbf{y}+\mathbf{e}\rangle .$$

Result : In the new basis, this results in X errors ! We use now a projective measurement according to the decomposition of the cosets of $\mathcal{C}_Z$

Simultaneous correction of X and Z errors

Same procedure

$$\frac{1}{\sqrt{2^{k_Z^\perp}}} \sum_{\mathbf{v} \in C_Z^\perp} |\mathbf{v} + \mathbf{w}\rangle \rightsquigarrow \frac{1}{\sqrt{2^{k_Z^\perp}}} \sum_{\mathbf{v} \in C_Z^\perp} (-1)^{(\mathbf{v}+\mathbf{w}).\mathbf{e}_2} |\mathbf{v} + \mathbf{w} + \mathbf{e}_1\rangle$$

where $e_1 \in \{0,1\}^n$ represents the X errors and e_2 the Z errors

Result : We can correct $\lfloor \frac{d_X - 1}{2} \rfloor$ errors de type X et $\lfloor \frac{d_Z - 1}{2} \rfloor$ errors of type Z, where d_X is the minimum distance of C_X and d_Z is the minimum distance of C_Z

Exercise

Compute (d_X, d_Z) for

1. the Steane code

2. the Shor code

Solution

1. $(d_X, d_Z) = (3, 3)$
2. $(d_X, d_Z) = (3, 2)$...

4. The stabilizer codes

4. The stabilizer codes

1. A class of codes containing the CSS codes
2. Many similarities with classical linear codes
3. Powerful framework for defining/manipulating/constructing/understanding quantum codes

The $\mathcal{G}_1$ error group

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

$\Rightarrow$ the elements of $\mathcal{G}_1$ commute or anti-commute

The $\mathcal{G}_n$ error group

- The elements of $\mathcal{G}_n$ commute or anti-commute

A simple criterion : $E_1 \dots E_n$ and $E'_1 \dots E'_n$ commute iff $\#\{i : E_i E'_i = -E'_i E_i\}$ is even

Example : XXI and XYX anti-commute and XXI and ZZZ commute

Definition

- Let $\mathcal{S}$ be an abelian subgroup of $\mathcal{G}_n$ where all the elements are of order 2 and $-1 \notin \mathcal{S}$, we call such a subgroup a stabilizer subgroup
- The stabilizer code $\mathcal{C}$ associated to $\mathcal{S}$ is the subspace of $\mathcal{H}^{\otimes n}$ defined by

$$\mathcal{C} = \{|\psi\rangle \in \mathcal{H}^{\otimes n} | \forall M \in \mathcal{S}, M |\psi\rangle = |\psi\rangle\}$$

Fundamental property

Proposition 1. *If the stabilizer subgroup is generated by $n-k$ independent generators, then the dimension of the quantum code is 2^k.*

Proof : by induction on $n-k$.

$n-k=1$, $\mathcal{S}=\{I,M\}$. The eigenvalues of M are ± 1. Let N be such that $NM=-NM$. We have

$$M\,|\psi\rangle = |\psi\rangle \Leftrightarrow MN\,|\psi\rangle = -N\,|\psi\rangle\,.$$

$\Rightarrow$ N swaps the eigenspaces associated to 1 and -1.
$\Rightarrow$ the two spaces have the same dimension, i.e 2^{n-1}.

$\mathcal{S}$ generated by j independent elements of order 2 $M_1, M_2, \ldots, M_j$
Induction hypothesis satisfied by $n - k = j - 1$
2 crucial arguments:

Lemma 1. *For a stabilizer group $\mathcal{S}$ generated by t generators of order 2 we have $|\mathcal{N}(\mathcal{S})| = 2^{2n+2-t}$.*

Lemma 2. *There exists $N \in \mathcal{G}_n$ that commutes with $M_1, \ldots, M_{j-1}$ and anti-commutes with M_j.*

Indeed, let $\mathcal{S}_t =< M_1, \ldots, M_t >$. $|\mathcal{N}(\mathcal{S}_{j-1})| = 2^{2n-j+3}$ then $|\mathcal{N}(\mathcal{S}_j)| = 2^{2n-j+2}$.

Let N commute with $M_1, \dots, M_{j-1}$ and anti-commute with M_j. Let

$$\begin{aligned} V &\stackrel{\text{def}}{=} \{|\psi\rangle : M_i |\psi\rangle = |\psi\rangle, 1 \le i \le j-1\} \\ V_1 &\stackrel{\text{def}}{=} \{|\psi\rangle : M_i |\psi\rangle = |\psi\rangle, 1 \le i \le j\} \\ V_2 &\stackrel{\text{def}}{=} \{|\psi\rangle : M_i |\psi\rangle = |\psi\rangle, 1 \le i \le j-1, M_j |\psi\rangle = -|\psi\rangle\} \end{aligned}$$

We have

$$V = V_1 \oplus V_2 \text{ and } NV_1 = V_2.$$

Therefore $\dim V_1 = \frac{\dim V}{2} = 2^{n-j}$.

Syndrome

For $E, F \in \mathcal{G}_n$ we denote by

$$E \star F \stackrel{\text{def}}{=} 0 \text{ if } E \text{ and } F \text{ commute and } 1 \text{ else}$$

for a choice $M_1, \dots, M_{n-k}$ of generators of $\mathcal{S}$ the syndrome associated to $E \in \mathcal{S}$ is

$$\sigma(E) \stackrel{\text{def}}{=} (M_i \star E)_{1 \leq i \leq n-k}$$

Syndrome (II)

- syndrome can be obtained by a measurement.
- Let $s \in \{0,1\}^{n-k}$, there exists $E(s)$ of syndrome s.
- Let $\mathcal{C}$ be the code stabilized by $\mathcal{S}$ and $\mathcal{C}(s) \stackrel{\text{def}}{=} E(s)C$. We have

$$\begin{aligned} \mathcal{C}(s) &= \{|\psi\rangle : M_i |\psi\rangle = (-1)^{s_i} |\psi\rangle\} \\ \mathcal{H}^{\otimes n} &= \overset{\perp}{\bigoplus}_{s \in \{0,1\}^{n-k}} \mathcal{C}(s) \end{aligned}$$

Analogies

Linear codes	stabilizer codes
k bits encoded in n bits	k qubits encoded in n qubits
subs. of dimension k	subs. of dimension 2^k
parity-check matrix $\mathbf{H}$	generator set of $\mathcal{S}$
$n-k$ rows, n columns	$n-k$ generators of $\mathcal{G}_n$
syndrome $\in \{0,1\}^{n-k}$	syndrome $\in \{0,1\}^{n-k}$

Decoding

- Decoding steps
  - Computing the syndrome by a projective measurement : quantum step
  - Determining the most likely error : classical step
  - Inverting the error : quantum step

Decoding(II)

- For a stabilizer code $\mathcal{C}$ associated to $\mathcal{S} =< S_1, \dots, S_{n-k} >$ we can distinguish two types of errors with 0 syndrome
  - those which belong to $\mathcal{S}$ (type **G**), such an error E is harmless: for all $|\psi\rangle \in \mathcal{C}$ we have $E|\psi\rangle = |\psi\rangle$
  - those which do not belong to $\mathcal{S}$ (type **B**), such an error E is harmful: it is impossible that $E|\psi\rangle = |\psi\rangle$ for all $|\psi\rangle \in \mathcal{C}$

Minimum distance and error correction capacity

- Minimum distance

$$d \stackrel{\text{def}}{=} \min\{|E| : E \text{ of type } \mathbf{B}\}$$

- Error correction capacity

$$\left\lfloor \frac{d-1}{2} \right\rfloor$$

- decoding success : $E_{\text{estimée}}^{-1} E_{\text{canal}}$ of type $\mathbf{G}$

Exercise : a first example

1. Let $\mathcal{C} = \text{Vect}(|000\rangle, |111\rangle)$. Show that this code is a stabilizer code

2. Determine the errors of $\mathcal{G}_3$ that are no detected by the code. Which are harmful? Which are harmless? What is the smallest error that can not be corrected ?

Exercise : a second example

Let

$$|\psi_0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$
$$|\psi_1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Show that the code generated by $|\psi_0\rangle|\psi_0\rangle|\psi_0\rangle$ and $|\psi_1\rangle|\psi_1\rangle|\psi_1\rangle$ is a stabilizer code. Give the set of errors of minimum weight that are not detected. Which are harmful ? Which are harmless ? What is the smallest error that can not be corrected ?

Exercise : revisiting Shor's code

1. Show that the Shor code is a stabilizer code
2. Show that there are errors of weight 1 that can be corrected without inverting the error. Determine all errors of this type
3. Did you experience the same phenomenon with the two previous codes?

Solution

1.

$$\begin{aligned}
\mathcal{S} &= <\mathcal{S}_X, \mathcal{S}_Z> \\
\mathcal{S}_X &= <XXXXXXIII, IIIXXXXXX> \\
\mathcal{S}_Z &= < H_Z > (\text{ generated by the rows of } H_Z \text{ }) \\
H_Z &= \begin{pmatrix} Z & Z & I & I & I & I & I & I & I \\ I & Z & Z & I & I & I & I & I & I \\ I & I & I & Z & Z & I & I & I & I \\ I & I & I & I & Z & Z & I & I & I \\ I & I & I & I & I & I & Z & Z & I \\ I & I & I & I & I & I & I & Z & Z \end{pmatrix}
\end{aligned}$$

2. The set of errors $\mathcal{E}$ of weight 1 is given by the rows of the matrix E

$$E = \begin{pmatrix} Z & I & I & I & I & I & I & I & I \\ I & Z & I & I & I & I & I & I & I \\ I & I & Z & I & I & I & I & I & I \\ I & I & I & Z & I & I & I & I & I \\ I & I & I & I & Z & I & I & I & I \\ I & I & I & I & I & Z & I & I & I \\ I & I & I & I & I & I & Z & I & I \\ I & I & I & I & I & I & I & Z & I \\ I & I & I & I & I & I & I & I & Z \end{pmatrix}$$

3. No

Exercise : CSS codes

1. Show that any CSS code is a stabilizer code
2. Give a set of stabilizers for the Steane code

Exercise : the 5 qubit code

Consider the stabilizer code associated to
$\mathcal{S} =< XZZXI, IXZZX, XIXZZ, ZXIXZ >$.

1. Show that every error in $\mathcal{G}_5$ of weight 1 or 2 has a syndrome $\neq 0$
2. Find a harmful error of weight 3
3. How many errors can be corrected by such a code ?
4. In which sense is this code better than Steane's code ?

Solution

1. $$\begin{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} & \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} \end{bmatrix}$$
2. $E = XXIZI$
3. 1
4. $R = \frac{1}{5} > \frac{1}{7}$

5. General error model

Exercise

Consider the stabilizer code on 3 qubits given by $\mathcal{S} =< ZZI, IZZ >$. Assume that the error is given by the unitary transform $U \otimes U \otimes U$ with

$$U = \begin{pmatrix} \cos\delta & i\sin\delta \\ i\sin\delta & \cos\delta \end{pmatrix}$$

with $\delta << 1$. What is the effect of the decoding algorithm we saw for this code?

General error model

Code correcting t errors and error unitary $T = (I + R)^{\otimes n}$ with $\|R\| \leq \epsilon$.

$$\begin{aligned} I + R &= (1 + O(\epsilon))I + O(\epsilon)X + O(\epsilon)Y + O(\epsilon)Z \\ T &= \sum_{A:|A|\leq t} R^{\otimes A} \otimes I^{\otimes \bar{A}} + \sum_{A:|A|>t} R^{\otimes A} \otimes I^{\otimes \bar{A}} \\ \sum_{A:|A|>t} R^{\otimes A} \otimes I^{\otimes \bar{A}} &\leq \sum_{j>t} \binom{n}{j} \|R\|^j = O(\epsilon^{t+1}) \end{aligned}$$