# Quelques codes quantiques

• Protéger l'information quantique contre les erreurs (lors de calcul, transmission, ou simplement durée).
• Importance cruciale pour le calcul quantique (un ordinateur classique n'a pas besoin de correction).
• Redondance (comme pour les codes classiques). Par exemple, on protège $k$ qubits, en utilisant $n$ qubits. Sous-espace de dimension $2^k$ dans $\mathbb{C}_2^{\otimes n} \simeq \mathbb{C}^{2^n}$.
• Calcul tolérant aux fautes : réaliser les portes logiques sur les états encodés.
• (Au moins) trois difficultés à priori : clonage impossible, erreurs continues, mesures nécessairement destructives.

■ **Quelques codes quantiques**



Un code quantique de paramètres $[[n, k]]$ est un sous-espace de dimension $2^k$ dans $\mathbb{C}^{2^n}$.

## 1. Les codes à répétition

### Le code *bit-flip*

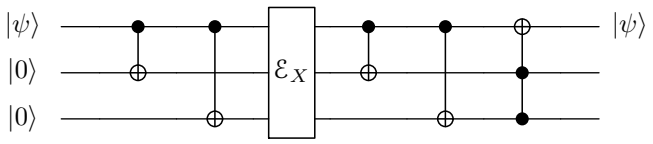
La façon la plus évidente de protéger l'information est de la dupliquer. Le clonage est impossible, mais l'opération

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longmapsto \alpha|00\cdots0\rangle + \beta|11\cdots1\rangle$$

est facilement réalisable. Par exemple, le code à répétition (*bit-flip*) de longueur 3 est engendré par les états

$$|\mathbf{0}\rangle_{\mathrm{BF}} = |000\rangle \qquad \text{et} \qquad |\mathbf{1}\rangle_{\mathrm{BF}} = |111\rangle.$$

Voici un circuit d'encodage/décodage sans mesures (la boîte $\mathcal{E}_X$ représente la zone où l'erreur peut survenir) :




Ce code permet de corriger une erreur de type $X$ (*bit-flip*). La partie décodage effectue une correction par majorité ; le qubit corrigé est obtenu en haut, et les deux autres sorties forment un syndrome de l'erreur (à noter que ce syndrome n'a même pas besoin d'être mesuré pour que la correction soit effectuée) :

$$\text{pas d'erreur : } |\psi00\rangle \qquad \text{erreur } X_1 : |\psi11\rangle \qquad \text{erreur } X_2 : |\psi10\rangle \qquad \text{erreur } X_3 : |\psi01\rangle.$$

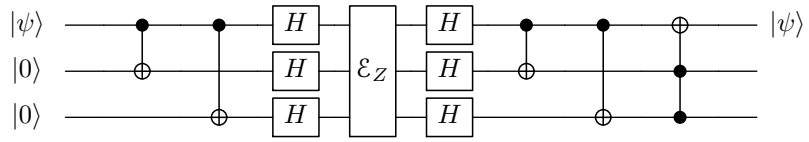
Notons que ce syndrome ne dépend que de l'erreur (comme il se doit), pas de $|\psi\rangle$. C'est parce que l'application de $\mathbb{F}_2^3$ dans $\mathbb{F}_2^2$ qui à un mot (éventuellement bruité) associe son syndrome est linéaire (elle est implémentée par les deux portes CNOT).

S'il se produit une erreur de type $Z$ (*phase-flip*), on obtient l'état $\alpha|000\rangle - \beta|111\rangle$ qui devient $\alpha|0\rangle - \beta|1\rangle$ après passage dans le circuit de correction. Donc l'erreur n'est **pas** corrigée.

Le code *bit-flip* de longueur 3 est aussi le sous-espace de $\mathbb{C}^8$ stabilisé par les opérateurs $ZZI$ et $IZZ$.

### Le code *phase-flip*

On peut transformer le code *bit-flip* en un code *phase-flip* (qui corrige une erreur de type $Z$) en l'encadrant avec une transformée de Walsh, implémentée par des portes de Hadamard.




Le code *phase-flip* est engendré par les états

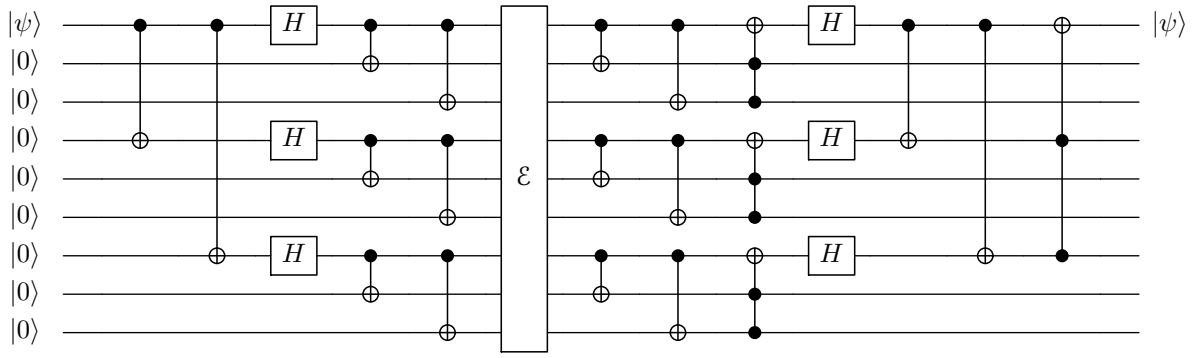
$$|\mathbf{0}\rangle_{\mathrm{PF}} = |+++\rangle = \frac{1}{\sqrt{8}} \sum_{a,b,c=0}^{1} |abc\rangle \qquad \text{et} \qquad |\mathbf{1}\rangle_{\mathrm{PF}} = |---\rangle = \frac{1}{\sqrt{8}} \sum_{a,b,c=0}^{1} (-1)^{a+b+c} |abc\rangle.$$

Il corrige une erreur $Z_1$, $Z_2$ ou $Z_3$. Il ne corrige pas les erreurs de type *bit-flip*.

Le code *phase-flip* est le code quantique stabilisé par les opérateurs $XXI$ et $IXX$.

## 2. Le code de Shor

Il consiste à emboîter un code *phase-flip* externe avec trois instances internes du code *bit-flip*. Le circuit de codage/décodage est alors




On obtient un code de paramètres $[[9, 1]]$. Les états $|0\rangle$ et $|1\rangle$ sont respectivement encodés en

$$|\mathbf{0}\rangle_{S9} = \frac{1}{\sqrt{8}}\big(|000\rangle + |111\rangle\big)^{\otimes 3} = \frac{1}{\sqrt{8}} \sum_{a,b,c=0}^{1} |aaabbbccc\rangle$$

$$|\mathbf{1}\rangle_{S9} = \frac{1}{\sqrt{8}}\big(|000\rangle - |111\rangle\big)^{\otimes 3} = \frac{1}{\sqrt{8}} \sum_{a,b,c=0}^{1} (-1)^{a+b+c} |aaabbbccc\rangle$$

où $abc$ représente un mot binaire. Les états $|+\rangle$ et $|-\rangle$ sont respectivement encodés en

$$|+\rangle_{S9} = \frac{1}{2}\big(|000000000\rangle + |000111111\rangle + |111000111\rangle + |111111000\rangle\big)$$
$$|-\rangle_{S9} = \frac{1}{2}\big(|111111111\rangle + |111000000\rangle + |000111000\rangle + |000000111\rangle\big)$$

Leurs images par la transformée de WH sont

$$|\widehat{+}\rangle_{S9} = \frac{1}{\sqrt{128}} \sum_{u,v,w=0}^{7} |uvw\rangle$$
$$|\widehat{-}\rangle_{S9} = \frac{1}{\sqrt{128}} \sum_{u,v,w=0}^{7} (-1)^{h(uvw)} |uvw\rangle$$

où les sommes sont restreintes à $h(u) \equiv h(v) \equiv h(w)$ modulo 2, avec $h(\cdot)$ poids de Hamming.

Le code de Shor est le sous-espace stabilisé par les opérateurs suivants :

| | | | |
|---|---|---|---|
| $ZZI\,III\,III$ | $III\,ZZI\,III$ | $III\,III\,ZZI$ | $XXX\,XXX\,III$ |
| $IZZ\,III\,III$ | $III\,IZZ\,III$ | $III\,III\,IZZ$ | $III\,XXX\,XXX$ |

L'opérateur $XXXIIIIII$ commute avec le stabilisateur. Il laisse donc le code (globalement) invariant (il est l'opérateur logique $Z_{S9}$) et forme une erreur non-triviale non détectable. La distance minimale du code de Shor est 3. Il y a des « erreurs » de poids 2 dans le stabilisateur, mais de ce fait, leur action est triviale. Le code S9 est dégénéré.

## Décodage

Le circuit décode $|\mathbf{0}\rangle_{S9}$ en $|000000000\rangle$ et $|\mathbf{1}\rangle_{S9}$ en $|100000000\rangle$, donc $|\psi\rangle_{S9}$ (tout état du code de Shor) en $|\psi\rangle_{S9}|0\rangle^8$.

Les erreurs $X_1$, $X_2$ et $X_3$ ont pour syndromes respectifs $|11\rangle_{23}$, $|10\rangle_{23}$ et $|01\rangle_{23}$. Je veux dire par là que $X_1|\psi\rangle_{S9}$ (par exemple) ressort du circuit de décodage sous la forme $|\psi\rangle_{S9}|11\rangle|000000\rangle$. Idem pour les autres $X_i$ dont les syndromes ont pour support les qubits $(5,6)$ ou $(8,9)$ au lieu de $(2,3)$.

Les erreurs $Z_1$, $Z_2$ et $Z_3$ ont même syndrome $|11\rangle_{47}$. Les autres $Z_i$ ont pour syndrome $|10\rangle_{47}$ et $|01\rangle_{47}$.

Toute erreur (un opérateur unitaire) sur un qubit peut s'écrire comme combinaison d'erreurs $X$ et $Z$ :

$$\begin{pmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{pmatrix} = \mathsf{re}(\alpha) I + \mathsf{im}(\beta) iX + \mathsf{re}(\beta) iY + \mathsf{im}(\alpha) iZ$$

où $\alpha, \beta \in \mathbb{C}$ avec $|\alpha|^2 + |\beta|^2 = 1$, et $Y = iXZ$. Donc le code de Shor permet de corriger une erreur quelconque (sur un unique qubit) !

## Code de Shor sur qudits

Le livre [9] présente, à la page 255, le code de Shor généralisé naturellement aux qudits. Pour les qutrits, il s'agit du code engendré par :

$$|u\rangle_T = \frac{1}{3\sqrt{3}}\big(|000\rangle + \omega^u|111\rangle + \omega^{2u}|222\rangle\big)^{\otimes 3}$$
$$= \frac{1}{3\sqrt{3}} \sum_{a,b,c=0}^{3} \omega^{u(a+b+c)} \, |aaabbbccc\rangle \qquad \text{pour } u = 0,1,2$$

et stabilisé par

$$\begin{array}{llll} ZZ^2I\,III\,III & III\,ZZ^2I\,III & III\,III\,ZZ^2I & XXX\,X^2X^2X^2\,III \\ IZZ^2\,III\,III & III\,IZZ^2\,III & III\,III\,IZZ^2 & III\,XXX\,X^2X^2X^2 \end{array}.$$

Ce code encode donc un qutrit en longueur 9.

L'article [29], pas très cohérent, prétend reprendre le code de Shor, mais définit plutôt celui, de dimension 27, engendré par

$$\begin{aligned} &|uvw\rangle_T \\ &= \frac{1}{3\sqrt{3}}\big(|000\rangle + \omega^u|111\rangle + \omega^{2u}|222\rangle\big) \otimes \big(|000\rangle + \omega^v|111\rangle + \omega^{2v}|222\rangle\big) \otimes \big(|000\rangle + \omega^w|111\rangle + \omega^{2w}|222\rangle\big) \\ &= \frac{1}{3\sqrt{3}} \sum_{a,b,c=0}^{3} \omega^{(ua+vb+wc)}\,|aaabbbccc\rangle \qquad \text{pour } u,v,w = 0,1,2 \end{aligned}$$

qui est stabilisé par

$$ZZZIIIIII,\quad IIIZZZIII,\quad IIIIIIZZZ,\qquad \omega^2XXXIIIIII,\quad \omega^2IIIXXXIII,\quad \omega^2IIIIIIXXX.$$

Je pose

$$\begin{aligned} |+\rangle_T &= \frac{1}{\sqrt{3}}\big(|0\rangle_T + |1\rangle_T + |2\rangle_T\big) = \frac{1}{3}\sum_{a+b+c\equiv 0} |aaabbbccc\rangle \\ |/\rangle_T &= \frac{1}{\sqrt{3}}\big(|0\rangle_T + \omega|1\rangle_T + \omega^2|2\rangle_T\big) = \frac{1}{3}\sum_{a+b+c\equiv 2} |aaabbbccc\rangle \\ |\backslash\rangle_T &= \frac{1}{\sqrt{3}}\big(|0\rangle_T + \omega^2|1\rangle_T + \omega|2\rangle_T\big) = \frac{1}{3}\sum_{a+b+c\equiv 1} |aaabbbccc\rangle. \end{aligned}$$

On voit que le code de Shor est un code CSS (ternaire) pour le code classique $C_1$ formé des mots $aaabbbccc$ et $C_2$ le sous-code formé des même mots mais tels que $a+b+c \equiv 0$ modulo 3.

## Le code de Ruskai

L'opérateur sur deux qubits

$$E = \frac{1}{2}(I\otimes I + X\otimes X + Y\otimes Y + Z\otimes Z)$$

a pour vecteurs propres les quatre états de Bell, avec valeur propre $-1$ pour le singlet et $+1$ pour les trois autres. Il correspond donc à l'échange de ces deux qubits.

Le code de Ruskai est de longueur 9, comme celui de Shor, mais corrige les échanges de deux qubits, en plus des erreurs de Pauli sur un qubit. Il est engendré par

$$\begin{aligned} |\mathbf{0}\rangle_R &= \frac{1}{2}\big(|000000000\rangle + \frac{1}{\sqrt{28}}\sum_\sigma |000111111\rangle\big) \\ |\mathbf{1}\rangle_R &= \frac{1}{2}\big(|111111111\rangle + \frac{1}{\sqrt{28}}\sum_\sigma |111000000\rangle\big) \end{aligned}$$

où les sommes sont sur les $\binom{9}{3} = 84$ permutations $\sigma$ permettant d'obtenir tous les mots de poids 6 (respectivement 3).

## 3. Codes CSS

La plupart des codes quantiques étudiés sont des codes Calderbank-Shor-Steane (CSS). Soient $C_2 \subseteq C_1$ deux codes linéaires binaires de longueur $n$. Le code CSS correspondant est le sous-espace $\mathcal{Q}$ de $\mathbb{C}^{2^n}$ engendré par les mots

$$|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle \qquad \text{où } x \in C_1. \tag{1}$$

Ces mots $|x + C_2\rangle$ et $|x' + C_2\rangle$ sont égaux si $x \equiv x'$ modulo $C_2$, et sont orthogonaux dans le cas contraire. La dimension de $\mathcal{Q}$ est $[C_1 : C_2] = 2^{k_1 - k_2}$ (où les $k_i$ sont les dimensions des $C_i$). C'est donc un code quantique de paramètres $[[n, k_1 - k_2]]$.

Il peut être plus clair de poser $C_1 = C_Z$ et $C_2 = C_X^\perp$. La condition initiale devient $C_X^\perp \subseteq C_Z$, ou encore $C_X^\perp \perp C_Z^\perp$ ou encore, en termes de matrices de contrôle, $H_X \cdot H_Z^T = 0$. Le nombre de qubits logiques $k$ est alors donné par $k = k_X + k_Z - n$, où $k_X$ et $k_Z$ sont les dimensions de $C_X$ et $C_Z$.

Pour $w = (w_1, \dots, w_n) \in \mathbb{F}_2^n$, on note

$$Z^w = Z^{w_1} \otimes \cdots \otimes Z^{w_n} \qquad \text{et} \qquad X^w = X^{w_1} \otimes \cdots \otimes X^{w_n}.$$

On peut voir que, pour $u, v, w \in \mathbb{F}_2^n$,

$$Z^u X^v = (-1)^{u \cdot v} X^v Z^u \tag{2}$$

et

$$H^{\otimes n} Z^w H^{\otimes n} = X^w \qquad \text{et} \qquad H^{\otimes n} X^w H^{\otimes n} = Z^w.$$

Par construction, les mots (1) sont stables par l'action des opérateurs $X^w$ pour $w \in C_X^\perp$, et aussi par l'action des opérateurs $Z^w$ pour $w \in C_Z^\perp$.

• Le code *bit-flip* est le code CSS obtenu avec $C_1 = \{000, 111\}$ et $C_2 = \{000\}$.

• Le code *phase-flip* est le code CSS obtenu avec $C_1 = \mathbb{F}_2^3$ et $C_2$ formé de tous les mots de poids pair.

• Si $C_1$ est le code classique formé des mots binaires de la forme *aaabbbccc*, et $C_2$ le sous-code formé des mots de $C_1$ de poids pair, le code CSS obtenu est le code de Shor.

### Action de la transformée de Walsh-Hadamard

Transformée WH sur $n$ qubits (de matrice $H^{\otimes n}$) :

$$|t\rangle \longmapsto \frac{1}{\sqrt{2^n}} \sum_{s \in \mathbb{F}_2^n} (-1)^{s \cdot t} |s\rangle.$$

**3.1.** — **Théorème.** *Soit $C$ un code linéaire binaire de longueur $n$ et $C^\perp$ son orthogonal dans $\mathbb{F}_2^n$. La transformée de Walsh-Hadamard de l'état*

$$|w\rangle = \frac{1}{\sqrt{|C|}} \sum_{t \in C} |t\rangle \qquad \textit{est donnée par} \qquad |\hat{w}\rangle = \frac{1}{\sqrt{|C^\perp|}} \sum_{s \in C^\perp} |s\rangle.$$

Démonstration — On a

$$\begin{aligned} |\hat{w}\rangle &= \frac{1}{\sqrt{|C|}} \sum_{t \in C} |\hat{t}\rangle = \frac{1}{\sqrt{|C|}} \sum_{t \in C} \frac{1}{\sqrt{2^n}} \sum_{s \in \mathbb{F}_2^n} (-1)^{s \cdot t} |s\rangle \\ &= \frac{1}{\sqrt{2^n |C|}} \sum_{s \in \mathbb{F}_2^n} \Big( \sum_{t \in C} (-1)^{s \cdot t} \Big) |s\rangle = \frac{1}{\sqrt{2^n |C|}} \sum_{s \in C^\perp} |C| |s\rangle \\ &= \sqrt{\frac{|C|}{2^n}} \sum_{s \in C^\perp} |s\rangle = \frac{1}{\sqrt{|C^\perp|}} \sum_{s \in c^\perp} |s\rangle \end{aligned}$$

parce que $s \cdot t = 0$ pour tout $t$ lorsque $s \in C^\perp$ et que l'application linéaire $C \ni t \mapsto s \cdot t \in \mathbb{F}_2$ a son noyau d'indice 2 dans $C$ lorsque $s \notin C^\perp$. □

Plus généralement, pour $x, z \in \mathbb{F}_2^n$, la transformée de l'état

$$\frac{1}{\sqrt{|C|}} \sum_{t \in C} (-1)^{t \cdot z} |t + x\rangle \qquad \text{est donnée par} \qquad \frac{(-1)^{x \cdot z}}{\sqrt{|C^\perp|}} \sum_{s \in C^\perp} (-1)^{s \cdot x} |s + z\rangle.$$

Tout état quantique stabilisé par un opérateur de la forme $P(Z)$ est envoyé, par la transformée de Walsh-Hadamard, sur un état quantique stabilisé par l'opérateur $P(X)$, et réciproquement. On en déduit que le code $\mathcal{Q} = \mathsf{CSS}(C_1, C_2)$ est transformé en code $\widehat{\mathcal{Q}} = \mathsf{CSS}(C_2^\perp, C_1^\perp)$.

## Capacité de correction

Soit $\mathcal{Q}$ le code CSS définit par les deux codes linéaires $C_X$ et $C_Z$ de longueur $n$, et donnés par les matrices de contrôle $H_X$ et $H_Z$. La matrice $H_Z$ attribue à chaque erreur un syndrome $s \in \mathbb{F}_2^{n-k_Z}$. L'espace $\mathbb{F}_2^n$ est la réunion disjointe des cosets $C_{Z,s}$ associés aux syndromes. Soit $\mathcal{Q}_s$ le sous-espace de $\mathbb{C}^{2^n}$ engendré par les $|w\rangle$ pour $w \in C_{Z,s}$. L'espace $\mathbb{C}^{2^n}$ est la somme directe et orthogonale des sous-espaces $\mathcal{Q}_s$. On peut donc envisager une mesure projective selon ces sous-espaces, dite *mesure de syndrome*.

Toute erreur $X^e$ (ou plus généralement $X^e Z^f$) envoie l'état initial $|\psi\rangle \in \mathcal{Q}$ dans $\mathcal{Q}_{s(e)}$ où $s(e)$ est le syndrome de $e$ pour $H_Z$. Si le code $C_Z$ a la capacité de corriger $e$ par syndrome, alors le code quantique $\mathcal{Q}$ a la capacité de corriger $X^e$. De la même façon, si le code $C_X$ a la capacité de corriger $f$ par syndrome, alors le code $\mathcal{Q}$ a la capacité de corriger $Z^f$.

En particulier, si $C_Z$ et $C_X$ sont $t$-correcteurs, alors le code quantique $\mathcal{Q}$ est $t$-correcteur, c'est-à-dire qu'il peut corriger toute erreur $X^e Z^f$ lorsque les poids de $e$ et $f$ sont $\leqslant t$.

## Distance minimale

**3.2. — Théorème.** *Soit $\mathcal{Q}$ le code CSS défini par les codes classiques $C_Z$ et $C_X$. On pose*

$$d_Z = \mathsf{min}\{\mathsf{wt}(w) \mid w \in C_Z \setminus C_X^\perp\} \qquad \textit{et} \qquad d_X = \mathsf{min}\{\mathsf{wt}(w) \mid w \in C_X \setminus C_Z^\perp\}.$$

*Alors la distance minimale de $\mathcal{Q}$ est $d = \mathsf{min}(d_Z, d_X)$.*

Démonstration — Une erreur de type $X^w$ est non-détectable si et seulement si $w \in C_Z$. Elle est triviale si et seulement si $w \in C_X^\perp$. Donc $d_Z$ est le poids minimal d'une erreur en $X$ non-triviale et non-détectable. Toute erreur se décompose en une erreur en $X$ et une erreur en $Z$. Pour un code CSS les deux types d'erreur sont détectés indépendamment. □

On note les paramètres d'un code quantique sous la forme $[[n, k, d]]$.

La base de $\mathcal{Q}$ formée des mots définis par (1) s'identifie au quotient de codes classiques $C_Z/C_X^\perp$, aussi noté $\mathcal{Q}_Z = C_{H_Z}^\perp/C_{H_X}$ par certains auteurs (les éléments de $\mathcal{Q}_Z$ peuvent s'identifier aux $Z$-opérateurs logiques). On a aussi une base duale qui s'identifie à $C_X/C_Z^\perp$, parfois noté $\mathcal{Q}_X = C_{H_X}^\perp/C_{H_Z}$.

## Résumé des notations

- Les matrices $H_X$ et $H_Z$ contrôlent des codes classiques $C_X$ et $C_Z$.
- On a $H_X H_Z^T = 0$, c'est-à-dire $C_X^\perp \perp C_Z^\perp$.
- Le code est l'espace stabilisé par les $X^w$ avec $w \in C_X^\perp$ et les $Z^w$ avec $w \in C_Z^\perp$.
- Le code est globalement stable sous les opérateurs $X^w$ avec $w \in C_Z$ et les $Z^w$ avec $w \in C_X$.
- Le poids minimal d'un opérateur non-trivial en $X$ est $d_Z$ et celui d'un opérateur non-trivial en $Z$ est $d_X$.

## 4. Le code de Steane

C'est le code quantique CSS basé sur le code de Hamming $[7,4,3]$ et son dual.

### Le code de Hamming

Le code $C$ de Hamming $[7,4,3]$ a pour matrices génératrice et de contrôle (en binaire et en hexadécimal) :

$$G = \begin{pmatrix} 1&0&0&0&0&1&1\\ 0&1&0&0&1&0&1\\ 0&0&1&0&1&1&0\\ 0&0&0&1&1&1&1 \end{pmatrix} = \begin{pmatrix} 43\\ 25\\ 16\\ 0\mathrm{f} \end{pmatrix} \qquad \text{et} \qquad H = \begin{pmatrix} 0&0&0&1&1&1&1\\ 0&1&1&0&0&1&1\\ 1&0&1&0&1&0&1 \end{pmatrix} = \begin{pmatrix} 0\mathrm{f}\\ 33\\ 55 \end{pmatrix}.$$

Il est faiblement auto-dual : son orthogonal $C^\perp$ engendré par $H$, de paramètres $[7,3,4]$, est contenu dans $C$. Le code $C^\perp$ est en fait le sous-code des poids pairs dans $C$. Le code $C$ est la réunion des cosets $C^\perp$ et $\mathbf{1}+C^\perp$ où $\mathbf{1} = (1111111)$.

### Le code de Steane

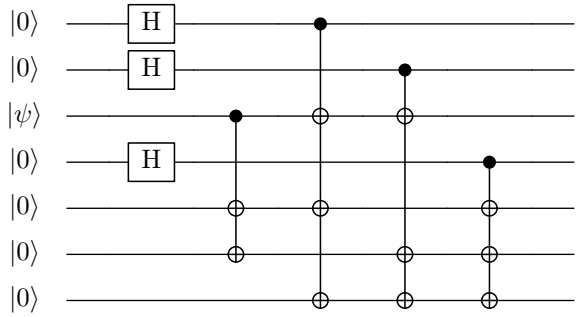
C'est le code CSS obtenu avec le code de Hamming pour $C_Z = C_X = C$. Il est engendré dans $\mathbb{C}^{2^7}$ par les deux mots (en hexadécimal) :

$$|\mathbf{0}\rangle_S = \frac{1}{\sqrt{8}} \sum_{t\in C^\perp} |t\rangle = \frac{1}{\sqrt{8}}\big(|00\rangle + |0\mathrm{f}\rangle + |33\rangle + |3\mathrm{c}\rangle + |55\rangle + |5\mathrm{a}\rangle + |66\rangle + |69\rangle\big)$$
$$|\mathbf{1}\rangle_S = \frac{1}{\sqrt{8}} \sum_{t\in C^\perp} |t+\mathbf{1}\rangle = \frac{1}{\sqrt{8}}\big(|7\mathrm{f}\rangle + |70\rangle + |4\mathrm{c}\rangle + |43\rangle + |2\mathrm{a}\rangle + |25\rangle + |19\rangle + |16\rangle\big).$$

Sa distance minimale est 3, c'est un code de type $[[7,1,3]]$.

### Encodage

Le qubit $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ est encodé en $|q\rangle_S = \alpha|\mathbf{0}\rangle_S + \beta|\mathbf{1}\rangle_S$. Voici un circuit d'encodage possible. La porte contrôlée par $|\psi\rangle$ contrôle l'addition de $|16\rangle \in C \setminus C^\perp$. Les trois portes contrôlées par les états $|+\rangle$ obtenus par les portes de Hadamard correspondent aux lignes de la matrice $H$ (génératrice de $C^\perp$).



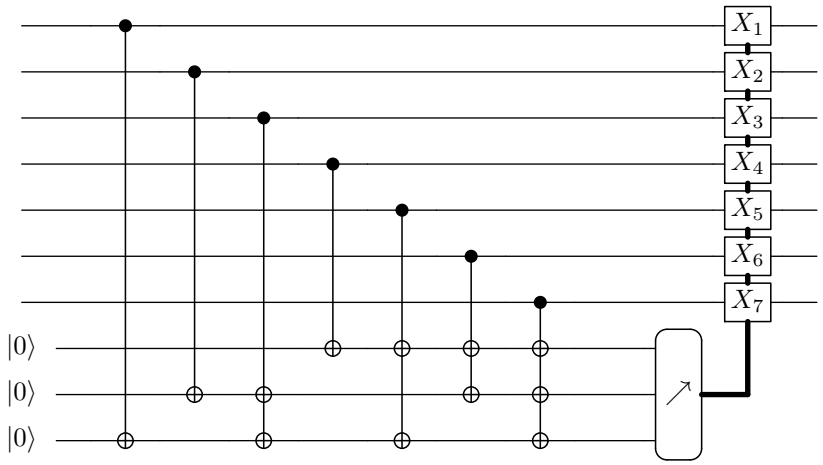

### Décodage

Par construction, le code de Steane est l'ensemble des états stables par les opérateurs

$$S_{Z2} = IIIZZZZ \qquad S_{X2} = IIIXXXX$$
$$S_{Z1} = IZZIIZZ \qquad S_{X1} = IXXIIXX$$
$$S_{Z0} = ZIZIZIZ \qquad S_{X0} = XIXIXIX$$

construits avec les lignes de $H$, et qui commutent deux-à-deux.

Si une erreur $X_i$ intervient (*bit-flip* sur le qubit $i$) alors la stabilité par les trois opérateurs en $Z$ ci-dessus est affectée. Plus précisément, pour $i = (i_2, i_1, i_0)_2$ on a $S_{Zj}|\psi\rangle = (-1)^{i_j}|\psi\rangle$. Il s'agit donc de déterminer le demi-syndrome $(i_2, i_1, i_0)$ et d'appliquer la correction $X_i$ indiquée. Cela peut se faire à l'aide du circuit suivant :




Si une erreur $Z_i$ intervient (*phase-flip* sur le qubit $i$), c'est le demi-syndrome correspondant aux trois opérateurs en $X$ qui est affecté. On peut corriger l'erreur en répétant le circuit de correction en $X$ après avoir intercalé une colonne de portes $H$ (qui réalisent une transformée de WH, transformant les erreurs $Z_i$ en $X_i$) entre les deux étages et à une autre à la fin.

La référence [13] propose un circuit qui procède différement. Son principe est général et utilise des circuits (9) pour calculer le syndrome. En fonction du syndrome mesuré, on applique la correction adéquate.

## Portes transversales

• Les opérateurs logiques *bit-flip* et *phase-flip* sont transversaux : $X_S = X^{\otimes 7} \sim IIXIXXI$ et $Z_S = Z^{\otimes 7} \sim IIZIZZI$. L'opérateur de Hadamard est aussi transversal : $H_S = H^{\otimes 7}$ (puisque les $S_{Zi}$ et $S_{Xi}$ sont échangés par cet opérateur, ainsi que le $Z_S$ avec $X_S$). On a $S_S^\dagger = S^{\otimes 7}$ où $S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$. Puisque $X_S$ est transversal et que le code de Steane est CSS, la porte contrôlée CX l'est aussi. Par contre, la porte $T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{smallmatrix}\right)$ n'est pas transversale.

## Action de Walsh-Hadamard

L'image du code de Steane par Walsh-Hadamard est le code engendré par

$$|\mathbf{0}\rangle_{\hat{S}} = \frac{1}{\sqrt{8}} \sum_{s \in C^\perp} |s\rangle = \frac{1}{4} \sum_{t \in C} |t\rangle = \frac{1}{\sqrt{2}} \big( |\mathbf{0}\rangle_S + |\mathbf{1}\rangle_S \big) = |+\rangle_S$$

$$|\mathbf{1}\rangle_{\hat{S}} = \frac{1}{\sqrt{8}} \sum_{s \in C^\perp} |s + \mathbf{1}\rangle = \frac{1}{4} \sum_{t \in C} (-1)^{h(t)} |t\rangle = \frac{1}{\sqrt{2}} \big( |\mathbf{0}\rangle_S - |\mathbf{1}\rangle_S \big) = |-\rangle_S$$

ce qui rappelle que le code de Steane est son propre orthogonal.

## Echange d'un bit de clé (avec le code de Steane)

Alice prépare l'état

$$|\mathcal{B}_y\rangle^{\otimes 7} = \frac{1}{\sqrt{128}} \sum_{r=0}^{127} |r\rangle \otimes |r\rangle$$

et envoie les parties droites (le $r$ de droite) à Bob. Alice et Bob font chacun une mesure de leurs qubits et obtiennent un mot de 7 bits, respectivement $a$ et $b$). Alice envoie $a + c$ à Bob où $c$ est pris au hasard dans

le code $C_1$ de Hamming. Bob corrige $a+b+c$ dans $C_1$, supprimant ainsi une éventuelle erreur $a+b$, et en déduit $c$. Le bit final est la classe de $c$ modulo $C_2$.

Variante avec ordinateurs quantiques : Alice applique $I\otimes H$ avec probabilité $1/2$ à l'état $|\mathcal{B}_y\rangle^{\otimes 7}$ et envoie la partie droite à Bob. Lorsque Bob a confirmé la réception, Alice lui précise si elle a appliqué $I\otimes H$. Si c'est le cas, Bob applique $H$ à sa partie pour reformer le $|\mathcal{B}_y\rangle^{\otimes 7}$ initial (plus ou moins altéré par l'environnement). Alice et Bob mesurent les syndromes quantiques de leurs parties respectives et comparent leurs résultats. Bob ajuste sa partie en appliquant des opérateurs de Pauli, pour que son syndrome devienne identique à celui mesuré par Alice. L'état obtenu (en négligeant les erreurs de poids $\geqslant 3$) est alors

$$\frac{1}{\sqrt{|C|}}\sum_{r\in x+C}|r\rangle\otimes|r\rangle=\frac{1}{\sqrt{2}}\big(|\mathbf{0}\rangle_S\otimes|\mathbf{0}\rangle_S+|\mathbf{1}\rangle_S\otimes|\mathbf{1}\rangle_S\big).$$

Alice et Bob peuvent en extraire un $|\mathcal{B}_y\rangle$ presque idéal et l'utiliser pour obtenir un bit de clé partagé.

## Cohérence collective de paires intriquées

Si on mesure les deux parties $|\mathcal{B}_y\rangle=\frac{1}{\sqrt{2}}\big(|00\rangle+|11\rangle\big)$ dans la même direction du plan $x,z$, on obtient la même issue (corrélation $+1$).

A partir d'un code CSS de longueur $n$, de qdim $k$ et de capacité de correction $t$, on peut obtenir $k$ paires $|\mathcal{B}_y\rangle$ avec grande fidélité en partant de $n$ paires imparfaites, pour peu que cette imperfection ne fasse pas apparaître plus de $t$ erreurs *bit flip* ni plus de $t$ erreurs *phase flip*.

Soit $Q$ un code CSS défini par les matrices de contrôle $H_X$ et $H_Z$ des codes classiques respectifs $C_X$ et $C_Z$ (donc $C_X^\perp\subseteq C_Z$). Pour $x,z\in\{0,1\}^n$, on peut définir le code quantique

$$Q_{x,z}:=\mathsf{phaseflip}_z\left(\mathsf{bitflip}_x(Q)\right)$$

qui est engendré par les

$$\pm\,\mathsf{phaseflip}_z\,\mathsf{bitflip}_x\,|v+C_X^\perp\rangle=\frac{1}{\left|C_X^\perp\right|}\sum_{w\in C_X^\perp}(-1)^{z\cdot w}|v+w+x\rangle\qquad\text{avec } v\in C_Z.$$

($Q_{x,z}$ est bien un code quantique, dont le stabilisateur est engendré par les mêmes générateurs que celui de $Q$, aux signes près.). Les éléments de $Q_{x,z}$ sont caractérisés par leur syndrome $(x,z)$ par rapport aux matrices $H_X$ et $H_Z$.

**4.1. — Propriété.** *Soit $P=\prod_I X_i\prod_J Z_j$ un opérateur de Pauli de longueur $n$. On suppose que Alice et Bob partagent un état $|\mathcal{B}_y\rangle^{\otimes n}$ et qu'ils mesurent chacun la valeur propre pour $P$ de leur partie respective. Alors ils obtiennent la même valeur $\in\{0,1\}$.*

Démonstration — Si Alice mesurait les $X_i$ (pour $i\in I$) et Bob aussi (mais ils ne le font pas), ils obtiendraient les mêmes valeurs $a_i=b_i$. De même pour les $Z_j$ (avec $j\in J$) ils obtiendraient $a'_i=b'_i$. Alice et Bob obtiennent donc pour $P$ la valeur

$$\prod_I a_i\prod_J a'_j=\prod_I b_i\prod_J b'_j$$

qui leur est commune. □

On peut appliquer ce même raisonnement à plusieurs opérateurs de Pauli qui commutent deux-à-deux. Donc si Alice et Bob mesurent chacun le syndrome sur l'état partagé $|\mathcal{B}_y\rangle^{\otimes n}$, ils obtiennent le même $(x,z)$ et l'état projeté après mesure du syndrome appartient à $Q_{x,z}\otimes Q_{x,z}$.

## 5. Codes stabilisateurs

### Groupe de Pauli

On note $\mathcal{P}_n$ l'ensemble des opérateurs de Pauli de longueur $n$ :

$$\mathcal{P}_n = \big\{u \cdot P_1 \otimes \cdots \otimes P_n \mid u \in \{\pm 1, \pm i\}, P_i \in \{I, X, Y, Z\}\big\}.$$

Ces opérateurs vérifient les propriétés suivantes :
• Ils sont à la fois unitaires et hermitiens (donc auto-inverses).
• Ils commutent deux-à-deux, ou anticommutent.
• Leurs valeurs propres sont $\pm 1$.
• Ceux obtenus pour la phase $u = 1$ forment une base de $\mathsf{End}(\mathbb{C}^{2^n})$.

**5.1. — Proposition.** *Soit $\mathcal{S}$ un sous-groupe de $\mathcal{P}_n$ ne contenant pas $-I$.*
*(a) On a $S^2 = I$ pour tout $S \in \mathcal{S}$.*
*(b) Le groupe $\mathcal{S}$ est abélien.*

Démonstration — (a) Puisque $X^2 = Y^2 = Z^2 = I$, on a $S^2 = \pm I$. Mais le signe $-$ est interdit.
(b) De même, pour $S, T \in \mathcal{S}$, on a $ST = \pm TS$. Mais si le signe est $-$ alors $STST = -STTS = -I \in \mathcal{S}$. □

#### Vecteurs d'exposants

À chaque élément $S$ de $\mathcal{P}_n$, on associe le double vecteur

$$e(S) = (x \mid z) \in \mathbb{F}_2^{2n} \qquad \text{pour } S = uX^xZ^z \text{ avec } u = \pm 1, \pm i. \tag{3}$$

D'après (2), deux opérateurs de Pauli $S$ et $S'$ tels que $e(S) = (x \mid z)$ et $e(S') = (x' \mid z')$ commutent si et seulement si le produit symplectique de ces doubles vecteurs s'annule :

$$xz' - x'z = 0. \tag{4}$$

D'autre part, on a l'identité

$$e(SS') = e(S) + e(S').$$

**5.2. — Proposition.** *Soient $S_1, \ldots, S_m$ des générateurs d'un sous-groupe $\mathcal{S}$ de $\mathcal{P}_n$ avec la condition $-I \notin \mathcal{S}$. Les $S_i$ forment un système générateur minimal (on ne peut pas lui enlever un élément) si et seulement si les $e(S_i) = (x_i \mid z_i)$ sont linéairement indépendants.*

Démonstration — Puisque $S_i^2 = I$ pour tout $i$, les éléments de $\mathcal{S}$ s'écrivent tous sous la forme $\prod_{j\in J} S_j$ où $J \subseteq \{1, \ldots, m\}$.

Les $(x_i \mid z_i)$ sont linéairement dépendants ssi il existe $J \neq \emptyset$ telle que $\sum_{j\in J}(x_j \mid z_j) = 0$, c'est-à-dire $\prod_{j\in J} S_j = I$ ou encore $S_{j_0} = \prod_{j\in J\setminus\{j_0\}} S_j$, c'est-à-dire $S_{j_0}$ redondant. □

Notons aussi que, inversement, si des $e_i = (x_i \mid z_i)$ sont linéairement indépendants (pour $1 \leqslant i \leqslant m$) et 2-à-2 orthogonaux pour le produit symplectique, on peut leur attribuer des $S_i$ tels que $e(S_i) = e_i$ et $S_i^2 = I$. Ils engendrent alors un groupe abélien d'ordre $2^m$.

**5.3. — Proposition.** *Soit $\mathcal{S}$ un sous-groupe de $\mathcal{P}_n$ ne contenant pas $-I$. On désigne par $\mathcal{Q}$ l'espace des états $|q\rangle$ tels que $S|q\rangle = |q\rangle$ pour tout $S \in \mathcal{S}$. On pose*

$$P = \frac{1}{|\mathcal{S}|} \sum_{S\in\mathcal{S}} S. \tag{5}$$

*(a) Alors $P$ est un projecteur hermitien.*
*(b) On a $P|q\rangle = |q\rangle$ si et seulement si $|q\rangle \in \mathcal{Q}$.*

*(c)* $\dim \mathcal{Q} = \operatorname{tr} P = 2^n/|\mathcal{S}|$.

Démonstration — (a) Chaque $S \in \mathcal{S}$ vérifie $S^\dagger = S^{-1} = S$. Donc $P$ est aussi hermitien. De plus,

$$P^2 = \frac{1}{|\mathcal{S}|^2} \sum_{S,T \in \mathcal{S}} ST = \frac{1}{|\mathcal{S}|} \sum_{U \in \mathcal{S}} U = P.$$

(b) Pour $|q\rangle \in \mathcal{Q}$, on a $S|q\rangle = |q\rangle$ pour tout $S \in \mathcal{S}$ donc $P|q\rangle = |q\rangle$. Réciproquement, si $P|q\rangle = |q\rangle$ alors, pour tout $S \in \mathcal{S}$, on a $SP = P$ donc $S|q\rangle = SP|q\rangle = P|q\rangle = |q\rangle$.

(c) On a d'une part $\dim \mathcal{Q} = \operatorname{rg} P = \operatorname{tr} P$ puisque $P$ est un projecteur. Mais dans la somme (5), il n'y a qu'un seul terme de trace non nulle : $\operatorname{tr} I = 2^n$. □

**5.4. — Corollaire.** *Soient $S_1, \ldots, S_m$ des éléments de $\mathcal{P}_n$ formant un système minimal. La dimension de l'espace des états $|q\rangle$ tels que $S_i|q\rangle = |q\rangle$ pour $1 \leqslant i \leqslant m$ est $2^{n-m}$.* □

## Codes stabilisateurs

C'est l'adaptation au monde quantique de la notion classique de code classique.

**5.5. — Définition.** Un code stabilisateur sur $n$ qubits est un sous-espace de $\mathbb{C}^{2^n}$ stabilisé par un sous-groupe $\mathcal{S}$ de $\mathcal{P}_n$ tel que $-I \notin \mathcal{S}$.

Un code stabilisateur est en général donné par une famille $(S_1, \ldots, S_m)$ de générateurs de $\mathcal{S}$ ou bien par la double matrice

$$H = (H_X \mid H_Z) = \big(e(S_i)\big)_{1 \leqslant i \leqslant m} \tag{6}$$

dont les lignes sout deux-à-deux orthogonales pour le produit symplectique (4), ce qui se traduit par

$$H_X H_Z^T - H_Z H_X^T = 0 \qquad (\text{dans } \mathbb{F}_2). \tag{7}$$

Si les $m$ générateurs sont indépendants, le sous-espace obtenu est de dimension $2^{n-m}$, d'après le corollaire 5.4. On dit alors que le code quantique est de dimension logique $n - m$.

Les codes CSS forment une sous-classe des codes stabilisateurs : celle qui correspond au cas où les $e(S_i)$ sont de la forme $(x_i \mid 0)$ ou $(0 \mid z_i)$. Les $x_i$ non nuls définissent alors le code $C_X^\perp$ et les $z_i$ non nuls définissent le code $C_Z^\perp$. La matrice (6) prend alors la forme

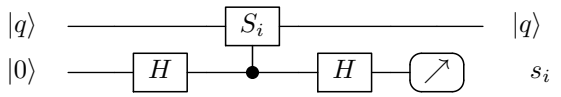
$$\left(\begin{array}{c|c} G_X & 0 \\ \hline 0 & G_Z \end{array}\right) \qquad \text{avec } G_X G_Z^T = 0. \tag{8}$$

### Syndromes

Pour $s = (s_1, \ldots, s_m) \in \mathbb{F}_2^m$, notons $\mathcal{Q}_s$ le sous-espace des kets $|q\rangle$ tels que

$$S_i|q\rangle = (-1)^{s_i}|q\rangle \quad \text{pour } 1 \leqslant i \leqslant m.$$

En particulier, le code est le sous-espace $\mathcal{Q}_0$. L'espace $\mathbb{C}^{2^n}$ est la somme directe et orthogonale des sous-espaces $\mathcal{Q}_s$. Un élément de $\mathcal{Q}_s$ est dit de *syndrome* $s$. Une mesure par rapport aux sous-espaces $\mathcal{Q}_s$ est une *mesure de syndrome*. On peut réaliser la mesure de chaque $s_i$ par le circuit suivant :

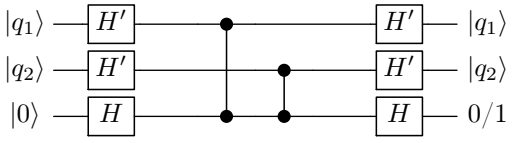



(9)

puisque la porte contrôlée appliquée à $|q\rangle \otimes |+\rangle$ donne $|q\rangle \otimes |(-1)^{s_i}\rangle$.

Dans les cas particuliers de syndromes d'opérateur en $X$ seulement, ou en $Z$ seulement, les circuits sont simplement :

ou bien encore




où les opérations $H'$ sont des $H$ dans le cas d'un syndrome en $X$, et des $I$ dans le cas d'un syndrome en $Z$.

### Syndrome d'une erreur

Soit $\mathcal{S}$ un sous-groupe de $\mathcal{P}_n$, ne contenant pas $-I$, engendré par les opérateurs $S_1, \ldots, S_m$ indépendants. On a une application qui à chaque erreur $E \in \mathcal{P}_n$ associe un $m$-uplet binaire :

$$\mathcal{P}_n \ni E \longmapsto s \in \mathbb{F}_2^m \quad \text{avec } ES_i = (-1)^{s_i} S_i E \tag{10}$$

qui est un homomorphisme de groupes. Ce $m$-uplet $s$ est aussi appelé le *syndrome* de l'erreur $E$ puisque, si l'erreur $E$ perturbe un état $|q\rangle$ du code, on a

$$S_i E|q\rangle = (-1)^{s_i} E S_i|q\rangle = (-1)^{s_i} E|q\rangle$$

c'est-dire $S_i|q'\rangle = (-1)^{s_i}|q'\rangle$ où $|q'\rangle = E|q\rangle$. Donc le syndrome de l'état $|q'\rangle$ est $s$. La mesure du syndrome de cet état perturbé permet donc de détecter l'erreur $E$, voire de la corriger en appliquant l'inverse d'une transformation de syndrome $s$.

Si une erreur est de syndrome nul mais n'appartient pas au stabilisateur $\mathcal{S}$, elle correspond à une erreur non détectable. La *distance minimale* $d$ d'un code stabilisateur est le poids minimal des erreurs de Pauli de syndrome nul bien que n'appartenant pas à $\mathcal{S}$. Si un état du code subit une erreur $E$ de poids $t < d/2$ alors un calcul de syndrome permet de détecter et corriger cette erreur.

### Dimension logique

**5.6. — Proposition.** *Si les $S_i$ pour $1 \leqslant i \leqslant m$ forment un système générateur minimal de $\mathcal{S}$ et si $-I \notin \mathcal{S}$ alors le code stabilisé par $\mathcal{S}$ encode $n - m$ qubits logiques.*

Démonstration — Les $e(S_i) = (x_i, z_i)$ forment une famille de rang $m$. La forme symplectique est non-dégénérée, donc les formes duales $\mu_i : (x, z) \mapsto x_i z + z_i x$ des $e(S_i)$ forment aussi une famille de rang $m$. Donc, pour tout $s = (s_i)_i \in \mathbb{F}_2^m$, il existe $(x, z) \in \mathbb{F}_2^{2n}$ tel que $\mu_i(x, z) = s_i$. Soit $S = X^x Z^z$, on a $SS_i = (-1)^{s_i} S_i S$ pour $1 \leqslant i \leqslant m$. Pour $|\psi\rangle$ de syndrome 0 par rapport aux $S_i$, on a $S|\psi\rangle$ de syndrome $s$. Donc les $2^m$ espaces associés aux différents syndromes ont tous même dimension $2^{n-m}$.

Alternativement, c'est une conséquence de la proposition 5.3. □

Cette démonstration montre aussi que, à partir de $m$ opérateurs stabilisateurs indépendants engendrant $\mathcal{S}$, on peut construire des opérateurs de Pauli $\hat{X}_i$, pour $1 \leqslant i \leqslant m$, vérifiant les relations de commutation (11), avec $\hat{Z}_i = S_i$. On peut donc en déduire l'existence d'un opérateur de Clifford qui envoie tout état de syndrome $s$ en un état de la forme $|q\rangle \otimes |s\rangle$. Décoder revient alors à extraire $|q\rangle$.

### Centralisateurs et normalisateurs

**5.7. — Rappels.** • Le centralisateur $\mathcal{C}(\mathcal{S})$ de $\mathcal{S}$ dans $\mathcal{P}_n$ est l'ensemble des $E \in \mathcal{P}_n$ tels que $SE = ES$ pour tout $S \in \mathcal{S}$. On a $\mathcal{S} \subseteq \mathcal{C}(\mathcal{S})$ puisque $\mathcal{S}$ est abélien.

• Le normalisateur de $\mathcal{S}$ dans $\mathcal{P}_n$ est l'ensemble des $E \in \mathcal{P}_n$ tels que $ESE \in \mathcal{S}$ pour tout $S \in \mathcal{S}$.

**5.8. — Lemme.** *Dans le groupe de Pauli $\mathcal{P}_n$, le centralisateur de $\mathcal{S}$ et le normalisateur de $\mathcal{S}$ sont égaux.*

Démonstration — • Si $E \in \mathcal{C}(\mathcal{S})$ alors, pour tout $S \in \mathcal{S}$, on a $SE = ES$ donc $ESE = S \in \mathcal{S}$. Donc $E$ est dans le normalisateur.

• Si $E \notin \mathcal{C}(\mathcal{S})$ alors $ESE = -S$ pour un $S \in \mathcal{S}$. Mais $-S \notin \mathcal{S}$ (puisque $-I \notin \mathcal{S}$). □

Relativement au groupe de Pauli, j'emploierai plus volontiers le terme de centralisateur. Je réserverai le terme de normalisateur, et je noterai $\mathcal{N}(\mathcal{S})$, pour le normalisateur de $\mathcal{S}$ dans le groupe des unitaires.

**5.9. — Propriété.** *Soit $\mathcal{S}$ un sous-groupe de $\mathcal{P}_n$ ne contenant pas $-I$ et soit $\mathcal{Q}$ le code stabilisé par $\mathcal{S}$. Pour $E \in \mathcal{P}_n$ On a $E\mathcal{Q} = \mathcal{Q}$ si et seulement si $E \in \mathcal{C}(\mathcal{S})$.*

Démonstration — • Supposons $E\mathcal{Q} = \mathcal{Q}$. Pour tout $|q\rangle \in \mathcal{Q}$ et $S \in \mathcal{S}$, on a $E|q\rangle \in \mathcal{Q}$ donc $SE|q\rangle = E|q\rangle$. Donc $ESE|q\rangle = |q\rangle$. On en déduit que $ESE \in \mathcal{S}$ et, en utilisant 5.8, que $E \in \mathcal{C}(\mathcal{S})$.
• Si $E \in \mathcal{C}(\mathcal{S})$ alors, pour tout $S \in \mathcal{S}$, on a $ESE = S$. Donc $ESE|q\rangle = |q\rangle$ pour tout $|q\rangle \in \mathcal{Q}$. Mais alors $SE|q\rangle = E|q\rangle$. Donc $E|q\rangle \in \mathcal{Q}$. On a ainsi montré $EQ \subseteq Q$. L'égalité s'ensuit puisque $E$ est unitaire. □

### Opérateurs logiques

**5.10. — Définition.** On dit qu'un opérateur unitaire $L$ est un *opérateur logique* pour le code de stabilisateur $\mathcal{S}$ lorsque $L \in \mathcal{N}(\mathcal{S})$.

Le normalisateur $\mathcal{N}(\mathcal{S})$ désigne ici l'ensemble des opérateurs **unitaires** $U$ sur $\mathbb{C}^{2^n}$ tels que $U^\dagger SU \in \mathcal{S}$ pour tout $S \in \mathcal{S}$.

**5.11. — Proposition.** *Tout opérateur logique $L$ du code $\mathcal{Q}$ stabilisé par $\mathcal{S}$ vérifie $L(Q) = Q$.*

Démonstration — • Si $L \in \mathcal{N}(\mathcal{S})$ alors, pour tout $S \in \mathcal{S}$, il existe $T \in \mathcal{S}$ tel que $L^\dagger SL = T$. On a alors $L^\dagger SL|q\rangle = T|q\rangle$ pour tout $|q\rangle \in \mathcal{Q}$. On obtient $SL|q\rangle = LT|q\rangle = L|q\rangle$ pour tout $S \in \mathcal{S}$, donc $L|q\rangle \in \mathcal{Q}$. □

Dans le cas particulier d'un opérateur $L$ qui est dans le groupe de Pauli $\mathcal{P}_n$, c'est un opérateur logique si et seulement si il appartient au centralisateur $\mathcal{C}(\mathcal{S})$ de $\mathcal{S}$ dans $\mathcal{P}_n$, en vertu du lemme 5.8.

**5.12. — Proposition.** *Soit $k = n - m$ le nombre de qubits logiques encodés. Le centralisateur $\mathcal{C}(\mathcal{S})$ est engendré par $\mathcal{S}$ et des opérateurs de Pauli $\hat{X}_i, \hat{Z}_i$ (avec $1 \leqslant i \leqslant k$) tels que*

$$\hat{X}_i\hat{X}_j = \hat{X}_j\hat{X}_i, \qquad \hat{Z}_i\hat{Z}_j = \hat{Z}_j\hat{Z}_i, \qquad \hat{X}_i\hat{Z}_j = (-1)^{\delta_{i,j}}\hat{Z}_j\hat{X}_i \qquad \text{pour tous } i, j. \tag{11}$$

Démonstration — Le stabilisateur $\mathcal{S}$ est engendré par $m = n - k$ générateurs indépendants. Son centralisateur $\mathcal{C}(\mathcal{S})$ est donc engendré par $n + k$ générateurs indépendants (ceux qui ont un $e(\cdot)$ orthogonal aux $e(S_i)$ pour le produit symplectique dans $\mathbb{F}_2^{2n}$). On peut choisir des générateurs de $\mathcal{S}$ pour $n - k$ d'entre eux. Il en reste $2k$ dont l'action logique est non-triviale. On peut en prendre $k$ (les $\hat{Z}_i$) qui commutent entre eux (qui stabilisent un seul état $|\hat{0^k}\rangle$). Trouver les $\hat{X}_i$ revient à diagonaliser la forme symplectique. □

### Distance minimale

**5.13. — Théorème.** *Soit $d$ le poids minimal des éléments de $\mathcal{C}(\mathcal{S}) \setminus \mathcal{S}$. Soit $t = \left\lfloor \frac{d-1}{2} \right\rfloor$. Toute erreur $E \in \mathcal{P}_n$ de poids $\leqslant t$ peut être corrigée.*

Démonstration — Soit $|q\rangle \in Q$ l'état encodé et $|q'\rangle = E|q\rangle$ l'état altéré, où $E$ est une erreur de poids $\leqslant t$. On peut calculer le syndrome $s$ de $|q'\rangle$. C'est aussi le syndrome de $E$. Parmi les erreurs, éléments de $\mathcal{P}_n$ de syndrome $s$, on choisit $E'$ de poids $t'$ minimal. Le syndrome de $E'E|q\rangle$ est $s + s = 0$. Donc $E'E \in \mathcal{C}(\mathcal{S})$. D'autre part $t' \leqslant t < d/2$, donc le poids de $E'E$ est $\leqslant t' + t < d$. Donc $E'E \in \mathcal{S}$. Finalement on peut retrouver $|q\rangle$ en appliquant $E'$ : $E'|q'\rangle = E'E|q\rangle = |q\rangle$. □

### Forme systématique

Tout code stabilisateur $[[n, k]]$ est équivalent à un code pour lequel la matrice (6) est sous forme systématique

$$\left(\begin{array}{ccc|ccc} I_r & A_1 & A_2 & B & 0 & C_1 \\ 0 & 0 & 0 & D & I_s & C_2 \end{array}\right) \tag{12}$$

qui s'obtient à partir de la matrice initiale par combinaisons de lignes et permutations identiques des deux colonnes au sein des deux moitiés. Les largeurs respectives des blocs de colonnes sont $(r, s, k, r, s, k)$ et on a $r + s + k = n$. On peut alors exprimer les $2k$ opérateurs logiques sous la forme

$$\left(\begin{array}{c} \hat{X} \\ \hat{Z} \end{array}\right) = \left(\begin{array}{ccc|ccc} 0 & C_2^T & I_k & C_1^T & 0 & 0 \\ 0 & 0 & 0 & A_2^T & 0 & I_k \end{array}\right).$$

## Erreurs corrigibles

**Le cas classique**

Pour un code binaire classique $C$ de longueur $n$, un ensemble d'erreurs $\mathcal{E}$ est une partie de $\mathbb{F}_2^n \times \mathbb{F}_2^n$ (le couple $(x, y)$ appartient à $\mathcal{E}$ si la sortie $y$ est possible lorsque l'entrée est $x$). L'exemple considéré le plus fréquemment est celui des erreurs de poids $\leqslant t$

$$\big\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid d(x, y) \leqslant t\big\}.$$

**5.14. — Définition.** On dit que l'ensemble $\mathcal{E}$ est corrigible lorsque :

$$\text{pour } x_1, x_2 \in C \text{ et } E_1, E_2 \in \mathcal{E}, \text{ on a} \qquad x_1 \neq x_2 \Rightarrow E_1(x_1) \neq E_2(x_2).$$

**Le cas quantique**

Pour un code quantique $\mathcal{Q} \subseteq \mathcal{H}$, un ensemble d'erreurs est une partie de $\mathsf{End}(\mathcal{H})$ (donc un ensemble d'opérateurs unitaires, ou non). Un exemple intéressant est celui des opérateurs dont le support (pour $\mathcal{H} = \mathcal{H}_2^{\otimes n}$) est de cardinal $\leqslant t$.

**5.15. — Définition.** On dit que l'ensemble $\mathcal{E}$ est corrigible lorsque :

$$\text{pour } |q_1\rangle, |q_2\rangle \in \mathcal{Q} \text{ et } E_1, E_2 \in \mathcal{E}, \text{ on a} \qquad |q_1\rangle \perp |q_2\rangle \Rightarrow E_1|q_1\rangle \perp E_2|q_2\rangle.$$

Remarquons dans ce cas que, pour $|w\rangle$ et $|w'\rangle$ éléments distincts de la base canonique, on a

$$\langle w|E_2^\dagger E_1|w'\rangle = \langle w'|E_2^\dagger E_1|w\rangle = \langle w + w'|E_2^\dagger E_1|w - w'\rangle = 0$$

ce qui entraîne $\langle w|E_2^\dagger E_1|w\rangle = \langle w'|E_2^\dagger E_1|w'\rangle$. On voit alors, que pour $|q_1\rangle$ et $|q_2\rangle$ non nécessairement orthogonaux, on a

$$\langle q_2|E_2^\dagger E_1|q_1\rangle = c(E_2^\dagger E_1)\,\langle q_2|q_1\rangle$$

où $c(E_2^\dagger E_1) \in \mathbb{C}$ est une constante.

**5.16. — Théorème.** *Soit $\{E_i\}_I$ un ensemble d'erreurs (opérateurs) de Pauli de longueur $n$. Si, pour tous $i, j \in I$ tels que $i \neq j$, on a $E_i^\dagger E_j \notin \mathcal{N}(\mathcal{S}) \setminus \mathcal{S}$ alors les erreurs $E_i$ forment un ensemble corrigible.*

## Opérateurs de Clifford

Le groupe de Clifford $\mathcal{C}\ell_n$ est le normalisateur du groupe de Pauli $\mathcal{P}_n$ dans $U(n)$, c'est-à-dire

$$\mathcal{C}\ell_n = \mathcal{N}(\mathcal{P}_n n) = \{C \in U(n) \mid CPC^\dagger \in \mathcal{P}_n, \forall P \in \mathcal{P}_n\}.$$

Ce groupe contient en particulier (en plus de $\mathcal{P}_n$) les portes $H$ et $S$, ainsi que les portes à deux qubits CNOT et SWAP. Tout automorphisme du groupe $\mathcal{P}_n$ est intérieur à $\mathcal{C}\ell_n$, c'est-à-dire de la forme $P \mapsto CPC^\dagger$ avec $C \in \mathcal{C}\ell_n$.

Le formalisme stabilisateur permet de spécifier des états quantiques comme points fixes d'opérateurs de Pauli. Si $|\psi\rangle$ est un état stabilisé par un opérateur $S \in \mathcal{P}_n$ alors $C|\psi\rangle$ est stabilisé par $S' = CSC^\dagger$. Puisque $S'$ est aussi un opérateur de Pauli (si $C \in \mathcal{C}\ell_n$) alors on peut remplacer les manipulations d'états quantiques par des manipulations de stabilisateurs. Ces manipulations sont plus aisées et les objets manipulés ont une représentation plus compacte.

Pour $n = 1$, le groupe de Pauli $\mathcal{P}_1$ contient 16 éléments (les 4 opérateurs de Pauli avec les 4 phases) et chaque opérateur de Clifford est caractérisé par son action de conjugaison sur $X$, $Y$ et $Z$ (sans tenir compte de la phase). Il s'identifie au groupe de symétries du cube. Il contient en particulier les rotations d'angle $\pi/4$ autour des trois axes $\frac{1}{\sqrt{2}}(I \pm iP)$, les rotations $\frac{1}{\sqrt{2}}(P \pm Q)$ d'angle $\pi/2$ autour d'une oblique (avec $P, Q = X, Y, Z$ distincts) dont la porte $H$, et les rotations $\frac{1}{2}(I \pm iX \pm iY \pm iZ)$ d'angle $2\pi/3$ autour d'une diagonale, dont la porte

$$V = \frac{1}{2}\begin{pmatrix} 1-i & -1-i \\ 1-i & 1+i \end{pmatrix}$$

dont l'action est $X \mapsto Y \mapsto Z \mapsto X$ et qui vérifie $V^3 = -I$. Pour $n$ quelconque, le groupe de Clifford est détaillé dans [17].

**5.17. — Théorème.** *Le groupe de Clifford est engendré (à phases globales près) par les portes $H$, $S$ et CNOT. Quantitativement, chaque élément de ce groupe peut être réalisé avec $O(n^2)$ exemplaires de ces portes.* □

Le formalisme stabilisateur permet en particulier d'échapper à la complexité exponentielle de la manipulation directe d'états de $n$ qubits. Les calculs dans ce formalisme sont donc facilement simulables par un ordinateur classique (c'est le théorème de Gottesman-Knill). Le potentiel supra-classique des ordinateurs quantique, s'il est avéré, devra mettre en œuvre des opérateurs non-Clifford, comme la porte $T$, ou bien la porte de Toffoli, ou bien encore la porte $S$ contrôlée (n'importe laquelle de ces trois portes est, accompagnée du groupe de Clifford, universelle pour le calcul quantique).

## Lien avec codes additifs sur $\mathbb{F}_4$

L'application définie par (3) peut être transportée sur $\mathbb{F}_4^n = \{0, 1, \alpha, \alpha^2\}$ en posant $\epsilon(S) = z + \alpha x$. Pour $\mathcal{S}$ sous-groupe de $\mathcal{P}_n$ ne contenant pas $-I$, l'ensemble $\{\epsilon(S) \mid S \in \mathcal{S}\}$ constitue un code $C$ additif sur $\mathbb{F}_4$. De plus, la condition (4) peut s'écrire $\epsilon(S)\epsilon(S')^* + \epsilon(S)^*\epsilon(S') = 0$, où $^*$ désigne la conjugaison $\alpha \leftrightarrow \alpha^2$. Il en résulte que le code $C$ est contenu dans son propre orthogonal pour cette forme trace. Inversement, un tel code additif et autodual définit un code quantique stabilisateur. On voit de plus que si il n'y a pas de vecteur non nul de poids $< d$ dans $C^\perp \setminus C$, alors la distance du code stabilisateur correspondant est (au moins) $d$.

## Conversion codes stabilisateurs / CSS

Réciproquement, à partir d'un code stabilisateur de matrice $(H_X \mid H_Z)$ (donc avec $H_X H_Z^T + H_Z H_X^T = 0$), on peut construire un code CSS de longueur et de dimension doublées, comme remarqué dans [24] (Theorem 1). Ce code est défini par

$$H' = \left(\begin{array}{c|c} G_X & 0 \\ \hline 0 & G_Z \end{array}\right) = \left(\begin{array}{c|c} H_X \mid H_Z & 0 \\ \hline 0 & H_Z \mid H_X \end{array}\right) \tag{13}$$

et la distance minimale résultante est au plus doublée.

## Intrication dans les codes stabilisateurs

Soit $Q$ un code quantique de longueur $n$ de groupe stabilisateur $\mathcal{S}$ de q-dimension $k$. On partitionne les $n$ qubits en deux groupes : $A \sqcup B = \{1, \ldots, n\}$ de cardinaux respectifs $n_A$ et $n_B$ (avec $n_A + n_B = n$). On peut alors écrire chaque $S \in \mathcal{S}$ sous la forme $S = S_A \otimes S_B$.

Si, pour chaque paire $S, T$ d'éléments de $\mathcal{S}$ les facteurs $S_A$ et $T_A$ commutent, alors notons $\mathcal{S}_A$ le groupe engendré par les $S_A$ (idem pour $\mathcal{S}_B$). Si aucun de ces deux groupes ne contient $-I$ alors on peut définir deux codes $Q_A$ et $Q_B$ de longueurs $n_A$ et $n_B$, et on a dans ce cas $Q_A \otimes Q_B \subseteq Q$. Plus généralement, on peut toujours trouver un vecteur $|q_A\rangle$ simultanément propre à tous les éléments de $\mathcal{S}_A$, et $|q_B\rangle$ de façon similaire pour $\mathcal{S}_B$. Et alors $|q_A\rangle \otimes |q_B\rangle \in Q$. Il en résulte que $Q$ contient des états non intriqués pour la partition $A \mid B$.

**5.18. — Proposition.** *Si au contraire, il existe $S, T \in \mathcal{S}$ qui anticommutent alors tous les états du code $Q$ sont intriqués (vis-à-vis des parties $A$ et $B$).*

Démonstration — Supposons que $Q$ contienne un état produit $|q\rangle = |q_A\rangle \otimes |q_B\rangle$ où $|q_A\rangle$ et $|q_B\rangle$ sont des états portés par les parties $A$ et $B$. On a

$$|q_A\rangle \otimes |q_B\rangle = |q\rangle = S|q\rangle = (S_A \otimes S_B)\big(|q_A\rangle \otimes |q_B\rangle\big) = S_A|q_A\rangle \otimes S_B|q_B\rangle.$$

Donc $S_A|q_A\rangle = \theta|q_A\rangle$ et $S_B|q_B\rangle = \theta^{-1}|q_B\rangle$ avec $|\theta| = 1$.

De la même façon $T_A|q_A\rangle = \theta'|q_A\rangle$ avec $|\theta'| = 1$. On en déduit que $S_A T_A|q_A\rangle = \theta\theta'|q_A\rangle = T_A S_A|q_A\rangle$ ce qui contredit l'affirmation que $S_A$ et $T_A$ anticommutent. □

### Codes stabilisateurs sur qudits

• Un code stabilisateur est un sous-espace de $\mathbb{C}_d^{\otimes n}$ stabilisé par un sous-groupe $\mathcal{S}$ de $\mathcal{P}_{n,d}$ qui ne contient aucun $\omega^k I$, sauf $I$. Dans le cas où $d$ n'est pas premier, on rajoute explicitement que $\mathcal{S}$ doit contenir **tous** les opérateurs de Pauli qui stabilisent le code.

**5.19. — Théorème [14].** *Soit $C$ un code stabilisateur de longueur $n$ sur des qudits. On a cette relation entre la dimension $K$ de $C$ et l'ordre du groupe stabilisateur $S$ :*

$$K \cdot |S| = d^n.$$

• *Si $d$ est composé, les générateurs de $\mathcal{S}$ peuvent avoir des ordres différents et l'ordre de $\mathcal{S}$ n'est pas nécessairement une puissance de $d$. Donc le nombre $k = \log_d K$ de qudits encodés n'est pas nécessairement entier.*
• *On généralise (3) : $e(\omega^t X^x Z^z) = (x \mid z) \in \mathbb{Z}_d^{2n}$.*
• *Pour $x, z \in \mathbb{Z}_d^n$, on a $Z^z X^x = \omega^? X^x Z^z$.*
• *Le produit symplectique (4) se généralise tel quel : $xz' - x'z \in \mathbb{Z}_d^{2n}$.*

• Un code stabilisateur peut corriger un ensemble $\mathcal{E}$ d'erreurs de Pauli si et seulement si, pour tous $E, F \in \mathcal{E}$, on a $E^\dagger F \notin \mathcal{C}(\mathcal{S}) \setminus \mathcal{S}$.

### Le code à trois qutrits $[[3, 1, 2]]_3$

C'est le code stabilisé par $XXX$ et $ZZZ$. Ses opérateurs logiques sont

$$\hat{X} = IXX^\dagger \qquad \text{et} \qquad \hat{Z} = Z^\dagger ZI.$$

C'est un code QMDS : $k + 2d = n + 2$. Il est linéairement engendré par

$$|\hat{0}\rangle = \frac{1}{\sqrt{3}}\big(|000\rangle + |111\rangle + |222\rangle\big), \quad |\hat{1}\rangle = \frac{1}{\sqrt{3}}\big(|012\rangle + |120\rangle + |201\rangle\big), \quad |\hat{2}\rangle = \frac{1}{\sqrt{3}}\big(|021\rangle + |210\rangle + |102\rangle\big).$$

Une erreur de type $X_i^x Z_j^z$ provoque un syndrome $(z, x)$ (indépendant de $i$ et $j$).

Ce code corrige un effacement : si un qutrit est perdu, on peut retrouver la valeur logique en évaluant $Z^\dagger Z$ sur les deux qutrits restants. On peut en fait reconstruire le qutrit $|q\rangle$ à partir de l'état encodé $|\hat{q}\rangle$, en appliquant une transformation unitaire sur seulement deux qubits (par exemple les deux premiers) :

$$(U_{A,B} \otimes I_C)|\hat{q}\rangle = |q\rangle_A \otimes \frac{1}{\sqrt{3}}\big(|00\rangle + |11\rangle + |12\rangle\big)_{B,C} \qquad \text{avec} \qquad U_{A,B} : |a, b\rangle \longmapsto |b - a, -a - b\rangle.$$

Par contre, si deux qutrits sont perdus, la valeur du qutrit restant n'apporte aucune information sur le qutrit restant. On a donc un schéma de partage de secret de type « 2 parmi 3 ».

## 6. Le code parfait à cinq qubits

C'est le code quantique dont le stabilisateur est engendré par $S_0 = IXZZX$ et ses permutés circulaires (seuls 4 sont indépendants). Il est engendré par

$$|\mathbf{0}\rangle_V = \frac{1}{4}\big(|00000\rangle + \sum_{i=0}^{4} \sigma^i|10100\rangle - \sum_{i=0}^{4} \sigma^i|11000\rangle - \sum_{i=0}^{4} \sigma^i|11110\rangle\big)$$
$$|\mathbf{1}\rangle_V = \frac{1}{4}\big(|11111\rangle + \sum_{i=0}^{4} \sigma^i|01011\rangle - \sum_{i=0}^{4} \sigma^i|00111\rangle - \sum_{i=0}^{4} \sigma^i|00001\rangle\big)$$

où $\sigma$ représente la permutation circulaire. Avec cette représentation, les opérateurs logiques élémentaires sont transversaux :

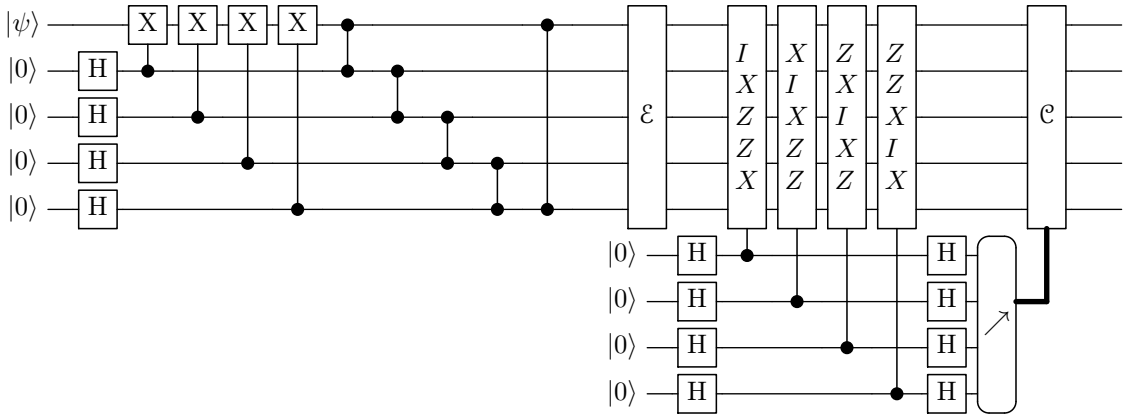
$$X_V = XXXXX \qquad \text{et} \qquad Z_V = ZZZZZ.$$

Les erreurs de poids 1 ont pour syndromes respectifs (donnés en hexadécimal) :

| | | |
|---|---|---|
| $Z_1$ : 4 (01001) | $X_1$ : 3 (00110) | $Y_1$ : 7 (01111) |
| $Z_2$ : a (10100) | $X_2$ : 1 (00011) | $Y_2$ : b (10111) |
| $Z_3$ : 5 (01010) | $X_3$ : 8 (10001) | $Y_3$ : d (11011) |
| $Z_4$ : 2 (00101) | $X_4$ : c (11000) | $Y_4$ : e (11101) |
| $Z_5$ : 9 (10010) | $X_5$ : 6 (01100) | $Y_5$ : f (11110) |

Les syndromes obtenus après deux erreurs sont aussi tous non nuls. Par contre il existe des erreurs de poids 3 qui stabilisent le code, par exemple $-IIZXZ = X_V \cdot S_0 \cdot \sigma(S_0)$. Ce code est donc de distance minimale 3 et son type est [[5,1,3]]. Il est stable par la permutation $Z \mapsto X \mapsto Y \mapsto Z$ : on a $\sigma^2(S_0) \cdot \sigma^3(S_0) = IYXXY$.

## Un circuit d'encodage et de correction




## Chiralité

Sous l'action de $H^{\otimes 5}$, on obtient un code équivalent, stabilisé par $IZXXZ$ et ses permutés circulaires, et engendré par

$$\frac{1}{4}\big(|00000\rangle + \sum_{i=0}^{4}\sigma^i|11000\rangle - \sum_{i=0}^{4}\sigma^i|10100\rangle - \sum_{i=0}^{4}\sigma^i|11110\rangle\big)$$

$$\frac{1}{4}\big(|11111\rangle + \sum_{i=0}^{4}\sigma^i|00111\rangle - \sum_{i=0}^{4}\sigma^i|01011\rangle - \sum_{i=0}^{4}\sigma^i|00001\rangle\big).$$

La permutation de qubits $P_{\times 2} : i \mapsto 2i$ modulo 5 est une autre façon de réaliser cette équivalence.

Le groupe d'automorphisme du code à 5 qubits est isomorphe au groupe diédral $D_5$, engendré par la permutation $\sigma$ et par le renversement de l'ordre des qubits.

## Portes logiques transversales

Les portes logiques simples (sur un seul qubit) de ce code sont transversales. On a déjà vu :

$$X_V = XXXXX \sim -IZXZI \qquad \text{et} \qquad Z_V = ZZZZZ \sim -XIZIX.$$

De plus, si on conjugue $S_0$ par $HHHHH$, on obtient $IZXXZ$ qui définit le code chiral. En composant par la permutation $P_{\times 2}$, on revient dans le code initial. Donc

$$H_V = P_{\times 2} \cdot HHHHH \qquad \text{et} \qquad K_V = KKKKK$$

où $K = SH = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ i & -i \end{smallmatrix}\right) \sim \mathsf{exp}\left(\frac{i\pi}{3} \cdot \frac{X+Y+Z}{\sqrt{3}}\right)$ a pour action par conjugaison $Z \mapsto Y \mapsto X \mapsto Z$ ; car on a aussi $P_{\times 2} \cdot SSSSS = S_V$.

La porte à deux qubits C-Z est aussi transversale [43]. Donc la porte C-X est aussi transversale. La porte $T$ ne l'est pas.

## Erreurs logiques

• Les opérateurs $E_0 = X_3$, $E_1 = Z_1$, $E_2 = Z_4$ et $E_3 = X_2$ forment une famille d'erreurs qui commutent entre elles et telles que $E_i S_j = (-1)^{\delta_{i,j}} S_j E_i$.

• On peut compléter les quatre générateurs du stabilisateur en cinq paires d'opérateurs logiques :

$$\begin{array}{lllll} \hat{Z}_1 = IXZZX & \hat{Z}_2 = XIXZZ & \hat{Z}_3 = ZXIXZ & \hat{Z}_4 = ZZXIX & \hat{Z}_5 = ZZZZZ \\ \hat{X}_1 = IZIZI & \hat{X}_2 = IIXXI & \hat{X}_3 = XXIII & \hat{X}_4 = ZIZII & \hat{X}_5 = XXXXX. \end{array}$$

## Forme systématique

Dans (12), on a $(r, \ell, k) = (4, 0, 1)$ et

$$(H_X|H_Z) \sim \left(\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{array}\right) \quad \text{pour} \quad \begin{array}{l} YZIZY \\ IXZZX \\ ZZXIX \\ ZIZYY \end{array}$$

puis

$$\left(\begin{array}{ccccc|ccccc} 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{array}\right) \quad \text{pour} \quad \begin{array}{l} \hat{X} = ZIIZX \\ \hat{Z} = ZZZZZ. \end{array}$$

## EPR

Soient $T_i$ (avec $0 \leqslant i \leqslant 4$) les cinq opérateurs obtenus par permutation cyclique de $IIZXZ$. On a $\prod_{i=0}^{4} T_i \sim X_V$. Pourtant $T_i|+\rangle_V = -|+\rangle_V$ pour chaque $i$ alors que $X_V|+\rangle_V = |+\rangle_V$. Ceci contredit une fois de plus le réalisme local.

## Partage de secret

On peut retrouver le bit encodé dans un état du code en mesurant l'opérateur $ZZZZZ$, ou bien par l'opérateur $ZZZZZ \cdot XIXZZ = -YZYII$ qui a l'avantage de restreindre son support aux trois premières parties. Il en résulte que trois parties (en fait n'importe lesquelles) peuvent déterminer le bit classique encodé. Par contre, si on « trace out » trois parties à un état du code, on obtient une densité $\frac{1}{4}I$ (c'est obligatoire puisque la distance du code est 3), donc deux parties seules ne peuvent retrouver aucune information sur le bit encodé. Plus convaincant pour moi, l'article [10] explique que, si deux parties pouvaient obtenir une information sur le mot encodé, alors une mesure potentielle leur permettrait de modifier l'état, ce qui est incompatible avec le fait que les trois autres parties peuvent obtenir le mot encodé à coup sûr.

## Lien avec le code de Hamming $[5, 3, 3]_4$.

Par la substitution $I \mapsto 0$, $X \mapsto 1$, $Z \mapsto \alpha$, $Y \mapsto \alpha^2 = 1 + \alpha$ on peut transformer les opérateurs de Pauli en mots sur $\mathbb{F}_4$. Le produit des opérateurs se traduit alors par l'addition des mots. Le stabilisateur du code à 5 qubits s'identifie alors aux combinaisons additives de $(0, 1, \alpha, \alpha, 1)$ et de ses permutés cycliques. En fait, ce mot et son permuté $(1, 0, 1, \alpha, \alpha)$ suffisent à engendrer le stabilisateur par $\mathbb{F}_4$-linéarité. On obtient la matrice de contrôle

$$\begin{pmatrix} 1 & 0 & 1 & \alpha & \alpha \\ 0 & 1 & \alpha & \alpha & 1 \end{pmatrix}$$

qui définit un code équivalent au code de Hamming sur $\mathbb{F}_4$, qui est plus couramment défini par la matrice de contrôle

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \alpha & \alpha^2 \end{pmatrix}.$$

## Borne de Hamming

Le code à 5 qubits est parfait : il atteint la borne de Hamming quantique présentée dans le théorème suivant.

**6.1. — Théorème.** *Soit $\mathcal{Q}$ un code quantique encodant $k$ qubits sur $n$ qubits capable de corriger toutes les erreurs affectant au plus $t$ qubits. On suppose de plus que $\mathcal{Q}$ est non dégénéré (les sous-espaces $E(\mathcal{Q})$, pour $E$ erreur correctible, sont deux-à-deux orthogonaux). On a la relation*

$$\sum_{i=0}^{t} \binom{n}{i} 3^i \leqslant 2^{n-k}.$$

Démonstration — Pour $0 \leqslant i \leqslant t$, il y a $\binom{n}{i}3^i$ erreurs de Pauli (en $X, Y, Z$) de poids $i$. La dimension de $\mathcal{Q}$ et de celle de chacun des sous-espaces $\mathcal{E}\mathcal{Q}$ est $2^k$. Puisque $\mathcal{Q}$ est supposé non dégénéré, on obtient $2^k \sum \binom{n}{i}3^i \leqslant 2^n$. □

## Le code à 5 qudits

Un exposé de Gottesman `http://pirsa.org/19110138` explique que le code à 5 qubits peut se généraliser aux qupits ($p$ premier) avec un stabilisateur engendré par $IXZZ^\dagger X^\dagger$ et ses permutés circulaires. Je ne sais pas si l'hypothèse $p$ premier est utile (pour que l'espace stabilisé par 4 générateurs indépendants et commutants soit de dimension $p$).

## Le groupe de Pauli (modulaire)

On pose $\omega = \mathsf{exp}(2i\pi/d)$ et on note

$$Z_d := \sum_{i=0}^{d-1} \omega^i |i\rangle\langle i| = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \omega & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & \omega^{d-1} \end{pmatrix} \qquad \text{et} \qquad X_d := \sum_{i=0}^{d-1} |i+1\rangle\langle i| = \begin{pmatrix} 0 & 0 & \cdots & 1 \\ 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 1 & 0 \end{pmatrix}$$

(les additions d'indices sont modulo $d$). Les matrices $X_d$ et $Z_d$ sont d'ordre $d$ et vérifient $Z_d X_d = \omega X_d Z_d$. Leurs valeurs propres sont les $d$ puissances distinctes de $\omega$. On pose aussi $H_d := \frac{1}{\sqrt{d}} \sum_{i,j} \omega^{ij} |i\rangle\langle j|$. On a

$$H^\dagger Z H = X \qquad \text{et} \qquad H^\dagger X H = Z^\dagger.$$

**6.2. — Proposition.** *Pour $d$ impair, je pose*

$$|t\rangle_s := \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{s\frac{j(j-1)}{2} - tj} |j\rangle.$$

*Pour $s, x, z \in \mathbb{Z}_d$ avec $x \neq 0$, on a*

$$X^x Z^z |t\rangle_s = \omega^{sx(x+1)/2 + x(t-z)} |t + xs - z\rangle_s.$$

*En particulier, les vecteurs propres de $X^x Z^z$ sont les $|t\rangle_s$ avec $s$ tel que $xs \equiv z$ modulo $d$.*

**6.3. — Proposition.** *Les deux opérateurs $P_1 = Z \otimes X$ et $P_2 = X \otimes Z$ commutent. L'espace invariant commun est la **droite** engendrée par le vecteur $\frac{1}{d} \sum_{i,j=0}^{d} \omega^{ij} |ij\rangle$.*

Démonstration — Les vecteurs propres pour $Z$ sont les $|t\rangle$ (pour $\omega^t$). Ceux pour $X$ sont les $|t\rangle' = \frac{1}{\sqrt{d}} \sum \omega^{-tj} |j\rangle$. L'espace invariant $E_1$ par $P_1$, et celui $E_2$ par $P_2$ sont respectivement engendrés par

$$|v_{1,t}\rangle := |t\rangle' \otimes |-t\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{tj} |t, j\rangle \quad \text{et} \quad |v_{2,t}\rangle := |-t\rangle \otimes |t\rangle' = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{tj} |j, t\rangle \qquad t = 0, \ldots, t-1.$$

Soit $|v\rangle \in E_1 \cap E_2$. Si $|v\rangle$ a une composante non nulle selon $|0,0\rangle$ (par exemple) alors il a le même coefficient selon les $|0,j\rangle$ et aussi selon les $|j,0\rangle$. On obtient alors $|v\rangle = \frac{1}{\sqrt{d}} \sum_t |v_{1,t}\rangle = \frac{1}{\sqrt{d}} \sum_t |v_{2,t}\rangle$. □

Le groupe (modulaire) de Pauli $\mathcal{P}_{n,d}$ est formé des

$$\omega^t \bigotimes_{i=1}^{n} X_d^{x_i} Z_d^{z_i}.$$

La phase $\omega^t$ importe peu et on cherche à s'en débarrasser, soit en ne manipulant que des générateurs dont les produits ne sont jamais égaux à $\omega^t I$ (sauf pour $t = 0$), ou soit en « ignorant » (quotientant) les phases (ce qui rend les produits commutatifs).

## 7. États graphes

À tout graphe $G$ à $n$ sommets on peut associer la liste des opérateurs $S_s = X_s \otimes \bigotimes_t Z_t$ où $s$ est un sommet de $G$ et $t$ décrit les voisins de $s$. Les $n$ opérateurs obtenus stabilisent un unique état, noté $|G\rangle$. Voir [20].

**7.1. — Théorème.** *L'état correspondant au graphe $G = (V, E)$ est donné par la formule :*

$$|G\rangle = \prod_{\{s,t\} \in E} Z_{i,j} |+\rangle^{\otimes n}$$

*où $Z_{s,t}$ désigne une porte $Z$ contrôlée entre les qubits $s$ et $t$.*

Démonstration — Par récurrence sur l'ensemble $E$. Pour un graphe sans arête, l'état stabilisé par les $S_v = X_v$ (où $v \in V$) est $|+\rangle^{\otimes n}$. Si $|q\rangle$ est stabilisé par les $S_u$ et qu'on rajoute (ou enlève) une arête $(s,t) \in E$ alors les opérateurs $S_s$ et $S_t$ deviennent :

$$S'_u = \left\{ \begin{array}{ll} S_u & \text{pour } u \neq s,t \\ Z_t S_u & \text{pour } u = s \\ Z_s S_t & \text{pour } u = t \end{array} \right\} = Z_{s,t} S_u Z_{s,t}.$$

Par exemple $Z_1 X_2 = Z_{1,2} X_2 Z_{1,2}$ :

$$\left(\begin{array}{c|c} I & 0 \\ \hline 0 & -I \end{array}\right) \left(\begin{array}{c|c} X & 0 \\ \hline 0 & X \end{array}\right) = \left(\begin{array}{c|c} X & 0 \\ \hline 0 & -X \end{array}\right) = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & Z \end{array}\right) \left(\begin{array}{c|c} X & 0 \\ \hline 0 & X \end{array}\right) \left(\begin{array}{c|c} I & 0 \\ \hline 0 & Z \end{array}\right).$$

Les $S_u$ sont donc conjugués par $Z_{s,t}$. Donc $Z_{s,t}|q\rangle$ est stabilisé par le nouveau graphe. □

**7.2. — Exemple.** Pour deux qubits, il y a deux graphes possibles. • Le graphe sans arête définit l'état produit $|+\rangle \otimes |+\rangle$ stabilisé par $XI$ et $IX$. Par actions locales d'opérateurs de Clifford (LC), on obtient les 36 états produits $|q_1\rangle \otimes |q_2\rangle$ avec $q_i \in \{0, 1, +, -, i, -i\}$.

• Le graphe connexe définit l'état maximalement intriqué

$$\frac{1}{2}\big(|00\rangle + |01\rangle + |10\rangle - |11\rangle\big) = \frac{1}{\sqrt{2}}\big(|0+\rangle + |1-\rangle\big)$$

stabilisé par $XZ$ et $ZX$. On obtient 24 états stabilisateurs par LC équivalence.

**7.3. — Exemple.** Pour $G$ graphe cyclique d'ordre 5, l'état correspondant est

$$\begin{aligned} |G\rangle = \frac{1}{\sqrt{32}}\big(|00000\rangle &+ \sum_{i=0}^{4} \sigma^i |10000\rangle - \sum_{i=0}^{4} \sigma^i |11000\rangle + \sum_{i=0}^{4} \sigma^i |10100\rangle \\ &+ \sum_{i=0}^{4} \sigma^i |11100\rangle - \sum_{i=0}^{4} \sigma^i |11010\rangle - \sum_{i=0}^{4} \sigma^i |11110\rangle - |11111\rangle\big). \end{aligned} \tag{14}$$

• Si $\Gamma$ est la matrice d'adjacence du graphe $G$ alors on peut aussi formuler

$$|G\rangle = \frac{1}{\sqrt{2^n}} \sum_{w \in \{0,1\}^n} (-1)^{\langle w|\Gamma|w\rangle/2} |w\rangle.$$

En effet, ajouter une arête $(s,t)$ à $G$, donc appliquer la porte controlée $Z_{s,t}$ à $|G\rangle$ change le signe des termes $w$ dont le support contient $s$ et $t$. Ceci est reflété par la valeur de $\langle w|\Gamma|w\rangle$ qui comptabilise deux 1 supplémentaires.

**7.4. — Proposition.** Soit $G$ un graphe à $n$ sommets on a, pour $1 \leqslant j \leqslant n$,

$$X_j|G\rangle = \Big( \prod_{k\in N(j)} Z_k \Big) |G\rangle$$

où $N(j)$ désigne l'ensemble des voisins de $j$ dans $G$.

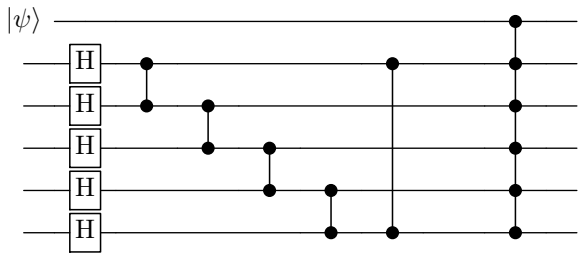
### Formalisme CWS

Les *Codeword Stabilizer Quantum Codes* sont présentés dans [11] et développés dans [23]. Le code CWS donné par un état graphe $|G\rangle$ et un code classique (non nécessairement linéaire) $C$ est l'espace engendré par les $Z^c|G\rangle$ où $c$ décrit $C$.

Par exemple, on peut prendre l'état graphe (14) défini par les cinq *codeword stabilizers* qui sont les permutés cycliques de $IIZXZ$. Pour $C$ code à répétition de longueur 5, les *codeword operators* sont $W_0 = IIIII$ et $W_1 = ZZZZZ$. On obtient un code quantique [[5,1]].

Toute erreur de poids 1 est équivalente à une erreur en $Z$ seulement ($X_i \sim Z_{i-1}Z_{i+1}$ et $Y_i \sim Z_{i-1}Z_iZ_{i+1}$). Aucune erreur de poids 2 n'est équivalente à $W$ donc les vecteurs $|G\rangle$ et $W|G\rangle$ sont séparés par des erreurs de poids $\geqslant 3$. Ils engendrent donc un code 1-correcteur. En fait $|G\rangle = \frac{1}{\sqrt{2}}\big(|\mathbf{0}\rangle_V - |\mathbf{1}\rangle_V\big)$ donc il s'agit exactement du code [[5,1,3]] décrit plus haut.

Pour l'encodage, on peut utiliser le circuit suivant, qui génère l'état $|G\rangle$, puis applique ensuite $W$ éventuellement (l'état $|0\rangle$ est encodé en $|-\rangle_V$ et l'état $|1\rangle$ est encodé en $|+\rangle_V$) :




Cette construction se généralise en toute longueur $n \geqslant 7$.

D'autre part, en remplaçant $W$ par les cinq permutés circulaires de $ZZIZI$, on obtient un code CWS (mais non stabilisateur) de paramètres $[[5, \mathsf{log}_2\, 6, 2]]$.

### Codes et états graphes

Voir [28].

## 8. D'autres codes

### Le code CSS de paramètres [[10,2,3]]

Il est obtenu à partir du code à cinq qubits par la construction (13). Son stabilisateur est engendré par

$$\begin{aligned} S_1 &= IXIIX\,IIXXI & S_5 &= IIZZI\,IZIIZ \\ S_2 &= XIXII\,IIIXX & S_6 &= IIIZZ\,ZIZII \\ S_3 &= IXIXI\,XIIIX & S_7 &= ZIIIZ\,IZIZI \\ S_4 &= IIXIX\,XXIII & S_8 &= ZZIII\,IIZIZ \end{aligned} \tag{15}$$

On peut associer

$$\begin{aligned} X_L &= X^{\otimes 5} \otimes I^{\otimes 5} & X_R &= I^{\otimes 5} \otimes X^{\otimes 5} \\ Z_L &= Z^{\otimes 5} \otimes I^{\otimes 5} & Z_R &= I^{\otimes 5} \otimes Z^{\otimes 5} \end{aligned}$$

aux deux qubits protégés. Les syndromes obtenus pour les différentes erreurs de poids 1 sont (en hexadécimal) :

| | | | | | |
|---|---|---|---|---|---|
| $Z_1 : 40$ | $X_1 : 03$ | $Y_1 : 43$ | $Z_6 : 30$ | $X_6 : 04$ | $Y_6 : 34$ |
| $Z_2 : \mathrm{a}0$ | $X_2 : 01$ | $Y_2 : \mathrm{a}1$ | $Z_7 : 10$ | $X_7 : 0\mathrm{a}$ | $Y_7 : 1\mathrm{a}$ |
| $Z_3 : 50$ | $X_3 : 08$ | $Y_3 : 58$ | $Z_8 : 80$ | $X_8 : 05$ | $Y_8 : 85$ |
| $Z_4 : 20$ | $X_4 : 0\mathrm{c}$ | $Y_4 : 2\mathrm{c}$ | $Z_9 : \mathrm{c}0$ | $X_9 : 02$ | $Y_9 : \mathrm{c}2$ |
| $Z_5 : 90$ | $X_5 : 06$ | $Y_5 : 96$ | $Z_{10} : 60$ | $X_{10} : 09$ | $Y_{10} : 69$ |

Ce code est de poids 3, car $S_1 S_2 X_L = IIIXI\,IIXIX$.

### Les codes de paramètres [[13,1,5]] et [[26,2,5]].

Le premier est le code stabilisé par $IIXZIIIIIIZXI$ et ses permutés circulaires. Le deuxième est la version CSS. Les contraintes en $X$ et $Z$ sont respectivement représentés par les matrices circulantes et définies par les polynômes palindromiques $X^t(1+X^{2t^2+1})$ et $X^{t+1}(1+X^{2t^2-1})$ modulo $X^{t^2+(t+1)^2}-1$ pour $t=2$. Le cas $t=1$ correspond aux codes [[5,1,3]] et [[10,2,3]]. Les cas généraux listés dans [24] (exemples 3 et 2) sont de paramètres $[[t^2+(t+1)^2, 1, 2t+1]]$ et $[[2t^2+2(t+1)^2, 2, 2t+1]]$.

### Les codes de Hamming quantiques

Le code de Steane se généralise en codes de Hamming quantiques, de paramètres $[[2^r-1, 2^r-1-2r, 3]]$. Ce sont les codes CSS obtenus à partir de $G_Z = G_X = H_r$ matrice de contrôle du code de Hamming classique d'ordre $r$.

On peut aussi définir une famille de codes $[[2^r, 2^r-r-2, 3]]$ non CSS avec une (double) matrice de contrôle basée sur deux exemplaires de $H_r$, dont le deuxième est permuté convenablement pour obtenir la condition d'orthogonalité (7), et munis de deux qubits de « parité ». Pour $r=3$ le code a pour paramètres [[8,3,3]] et pour matrice de contrôle

$$(H_X \mid H_Z) = \left(\begin{array}{c|c} 10100101 & 00001111 \\ 10101010 & 00110011 \\ 10010110 & 01010101 \\ 00000000 & 11111111 \\ 11111111 & 00000000 \end{array}\right)$$

et ses opérateurs logiques sont

$$\begin{aligned} \hat{Z}_1 &= IZIZIZIZ & \hat{X}_1 &= XXIIIZIZ \\ \hat{Z}_2 &= IIZZIIZZ & \hat{X}_2 &= XIXZIIZI \\ \hat{Z}_3 &= IIIIZZZZ & \hat{X}_3 &= XIIZXZII. \end{aligned}$$

### Le code de Reed-Muller $[[2^m-1, 1, 3]]$

Soit $G_Z$ la matrice à $m \geqslant 3$ lignes dont les colonnes sont les développement binaires des entiers de 1 à $2^m-1$ (elle contrôle le code de Hamming $[2^m-1, 2^m-m-1, 3]$). Soit $G_X$ une matrice génératrice du sous-code des poids pairs du code de Hamming, donc de rang $2^m-m-2$. On a $G_Z G_X^T = 0$. On obtient un code CSS par la construction (8). Pour $m=3$ c'est le code de Steane. Pour $m=4$ on obtient le code $[[15,1,3]]$ dont la porte logique $T$ est transversale.

## 9. Calcul quantique tolérant aux fautes et théorème du seuil

L'intérêt pratique d'un code quantique particulier est particulièrement augmenté s'il permet des calculs tolérants aux fautes. Cela veut dire que les portes logiques élémentaires peuvent être réalisées dans le domaine encodé en bloquant la propagation des erreurs. C'est en général le cas des portes transversales mais on peut obtenir aussi des portes tolérantes par des techniques utilisant des "états magiques" (états auxiliaires préparés en amont).

## Théorème du seuil

Si on note $p$ la probabilité qu'une porte physique élémentaire subisse une erreur, on peut obtenir par ces techniques une probabilité d'erreur $cp^2$ où $c$ est une constante du code (liée au nombre de possibilités d'apparition d'erreurs multiples, excédant la capacité de correction du code). Si $cp < 1$, on gagne en fiabilité à calculer dans le domaine encodé, par rapport au calcul direct.

Le théorème du seuil part de l'idée qu'on peut superposer en principe plusieurs couches d'encodage. Avec $k$ couches, la probabilité d'erreur est $p_k = (cp)^{2^k}/c$. Sous l'hypothèse $p < 1/c$ (la constante $1/c$ est appelée le *seuil* du code), on peut trouver $k$ tel que $p_k \leqslant \varepsilon/g(n)$ où $\varepsilon$ est la fiabilité (probabilité d'erreur max) souhaitée du calcul global et $g(n)$ le nombre de portes du circuit direct (dépend du nombre $n$ de qubits de l'entrée). La condition pour ce $k$ s'écrit

$$(cp)^{2^k} \leqslant \frac{\varepsilon c}{g(n)}$$

ou encore

$$2^k \leqslant \frac{\log\big(\varepsilon c/g(n)\big)}{\log(cp)}.$$

Si on note $d$ le facteur représentant le surcoût représenté par chaque couche d'encodage, en termes de nombre de portes traversées, le surcoût apporté par les $k$ couches vérifie

$$d^k \leqslant \left(\frac{\log\big(g(n)/\varepsilon c\big)}{\log(1/cp)}\right)^{\log d} \in O\Big(\log\big(g(n)/\varepsilon\big)^{\log d}\Big).$$

On obtient alors l'énoncé suivant :

**9.1. — Théorème.** *Soit $\varepsilon > 0$. Tout circuit initial à $g(n)$ portes quantiques peut être simulé par un circuit de probabilité d'erreur $< \varepsilon$ comportant*

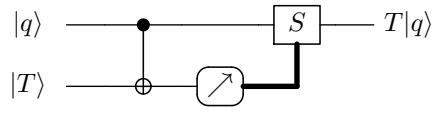
$$g(n) \cdot \mathrm{poly}\big(\log g(n)/\varepsilon\big)$$

*portes physiques, sous l'hypothèse que la probabilité $p$ d'erreur des portes élémentaires soit majorée par une constante seuil $1/c$ dépendant du code utilisé.*

En Août 2024, l'équipe quantique de Google annonce avoir implémenté un code surface avec $cp < 1$.

## États magiques

Pour de nombreux codes courants (le code parfait à 5 qubits, les codes CSS autoduaux, ...), les portes de Clifford peuvent être implémentées de façon transversale, donc tolérante aux fautes. C'est rarement le cas de la porte $T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \zeta \end{smallmatrix}\right)$, où $\zeta = \exp(i\pi/4)$. Pour celle-ci, on peut utiliser le circuit suivant

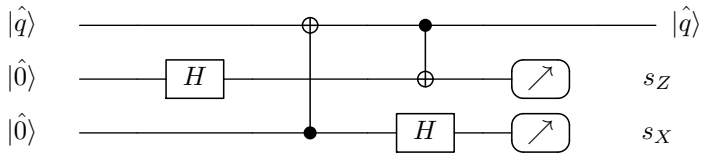



où l'état « magique » d'entrée est $|T\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + \zeta|1\rangle\big)$. L'état obtenu est $T|q\rangle$ à une phase globale près.

Ce circuit ne semble que déplacer le problème puisqu'on imagine à priori qu'il faut une porte $T$ pour préparer l'état $|T\rangle$. Mais en fait on peut fabriquer des états $T$ par diverses méthodes, la plus simple étant de faire une mesure (tolérante aux fautes !) d'un état $|0\rangle$ selon la base propre de l'opérateur $\zeta^* SX$ et de post-sélectionner les états correspondant à l'issue $+1$.

### Calcul de syndrome tolérant aux fautes

Pour calculer les syndromes d'un code CSS $\mathcal{Q}$ de façon tolérante aux fautes, on peut utiliser cette méthode dite de Steane. Elle peut être représentée par le circuit




où les états $|\hat{0}\rangle$ sont des $|0\rangle$ logiques encodés dans $\mathcal{Q}$ et où les quatre portes agissent dans le domaine encodé et sont implémentées de façon tolérante aux fautes.

Expliquons l'extraction de $s_Z$. L'entrée de la porte CNOT est $|\hat{q}\rangle \otimes |\hat{+}\rangle$. La sortie est inchangée si $|\hat{q}\rangle$ est sans erreur puisque $|+\rangle$ est invariant sous NOT. Si $|\hat{q}\rangle$ est entâché d'erreur *bit-flip*, son syndrome non-trivial est transféré dans le bloc ancilla. En faisant une mesure dans la base canonique, on obtient un mot classique portant ce même syndrome (parce que la valeur logique encodée dans l'ancilla est 0), que l'on peut obtenir en utilisant la matrice de contrôle du code de Hamming.

Pour $s_X$ c'est similaire. Si $|\hat{q}\rangle$ est sans erreur, l'ancilla est inchangée par la porte CNOT. Mais si $|\hat{q}\rangle$ est entâché d'une erreur *phase-flip*, son syndrome remonte la porte CNOT à contre-courant. Cette erreur éventuelle est ensuite convertie en erreur *bit-flip* avant mesure.

## 10. Les codes à jauge

C'est un espace stabilisé isomorphe à un produit $\mathcal{Q}_\mathcal{L} \otimes \mathcal{Q}_\mathcal{G}$ où seul le facteur de gauche est utilisé pour porter l'information quantique protégée. Il est défini par un sous-groupe $\mathcal{G}$ dit *de jauge* du groupe de Pauli $\mathcal{P}_n$ sur $n$ qubits. Le stabilisateur $\mathcal{S}$ est le centre de $\mathcal{G}$ (aux phases près : $-I \notin \mathcal{S}$). On a la situation globale suivante :

$$\langle i, \mathcal{S}\rangle = \mathcal{G} \cap \mathcal{C}(\mathcal{G}) \leqslant \mathcal{C}(\mathcal{S}) \leqslant \mathcal{P}_n$$

où $\mathcal{C}(\cdot)$ désigne les centralisateurs dans $\mathcal{P}_n$. Le groupe $\mathcal{C}(\mathcal{S})/\mathcal{S}$ est alors le groupe des opérateurs sur les qubits logiques (voir proposition 5.12), mais ceux-ci se répartissent en *qubits de jauge* (c'est-à-dire non utilisés) et en *qubits protégés*.

Les éléments de $\mathcal{C}(\mathcal{G})$ sont des opérateurs logiques qui agissent seulement sur les qubits protégés (*bare operators*). Ceux qui sont non-triviaux sont représentés par $\mathcal{C}(\mathcal{G}) \setminus \mathcal{S}$. Les éléments de $\mathcal{L} = \mathcal{C}(\mathcal{S})$ sont les *dressed operators*, qui agissent sur les qubits logiques (protégés et de jauge). Ceux qui ont une action non-triviale sur les qubits protégés sont représentés par $\mathcal{C}(\mathcal{S}) \setminus \mathcal{G}$. Le poids minimal de ces derniers est la distance minimale du code.

**10.1. — Proposition.** *(a) Le groupe $\mathcal{G}$ est engendré par $\mathcal{S}$ et des opérateurs $\hat{X}_i$ et $\hat{Z}_i$ (avec $1 \leqslant i \leqslant g$) tels que tout le monde commute sauf $\hat{X}_i\hat{Z}_i = -\hat{Z}_i\hat{X}_i$.*
*(b) Le groupe $\mathcal{L} = \mathcal{C}(\mathcal{S})$ est engendré par $\mathcal{C}(\mathcal{G})$ et $\mathcal{G}$. (Les dressed operators sont produits de bare operators et d'opérateurs de jauge.)*

Démonstration — (a) Similaire à la proposition 5.12 (mais seulement les $\hat{X}_i$ et $\hat{Z}_i$ de jauge sont invoqués). (b) Pour $C \in \mathcal{C}(\mathcal{S})$, posons $C\hat{X}_i = \varepsilon_i \hat{X}_i C$ et $C\hat{Z}_i = \eta_i \hat{Z}_i C$ avec $\varepsilon_i, \eta_i = \pm 1$. En posant $\hat{L} = \prod_{i=1}^{g} \hat{Z}_i^{\varepsilon_i} \hat{X}_i^{\eta_i} \in \mathcal{G}$ on obtient $C\hat{L} \in \mathcal{C}(\mathcal{G})$. □

### Le code de Bacon

C'est un code de longueur $d^2$ (avec $d \in \mathbb{N}^*$) et je le détaille pour $d = 3$. Il faut imaginer les $d^2$ qubits disposés dans un tableau $d \times d$. Soit $\mathcal{S}$ le sous-groupe de Pauli abélien engendré par les $2(d-1)$ opérateurs :

$$S_1 = \begin{pmatrix} XXX \\ XXX \\ \bullet\ \bullet\ \bullet \end{pmatrix}, \qquad S_2 = \begin{pmatrix} \bullet\ \bullet\ \bullet \\ XXX \\ XXX \end{pmatrix}, \qquad S_3 = \begin{pmatrix} ZZ\bullet \\ ZZ\bullet \\ ZZ\bullet \end{pmatrix}, \qquad S_4 = \begin{pmatrix} \bullet ZZ \\ \bullet ZZ \\ \bullet ZZ \end{pmatrix}. \tag{16}$$

Il stabilise un code quantique de dimension logique $d^2-2(d-1)=(d-1)^2+1=5$ qubits, engendré par les

$$\frac{1}{2}\left(\left|\begin{matrix}a_1a_2a_3\\b_1b_2b_3\\c_1c_2c_3\end{matrix}\right\rangle+\left|\begin{matrix}\bar a_1\bar a_2\bar a_3\\\bar b_1\bar b_2\bar b_3\\c_1c_2c_3\end{matrix}\right\rangle+\left|\begin{matrix}a_1a_2a_3\\\bar b_1\bar b_2\bar b_3\\\bar c_1\bar c_2\bar c_3\end{matrix}\right\rangle+\left|\begin{matrix}\bar a_1\bar a_2\bar a_3\\b_1b_2b_3\\\bar c_1\bar c_2\bar c_3\end{matrix}\right\rangle\right)\qquad\begin{matrix}\text{avec les trois colonnes}\\\text{de même parité.}\end{matrix}\tag{17}$$

Ce code est de poids minimal 2 puisque il existe des opérateurs de poids 2 (les « fragments » ci-dessous) qui commutent avec $\mathcal{S}$ et donc dont l'action ne change pas les syndromes. Pour obtenir un code ayant de bonnes capacités de correction, il faut diminuer la dimension du code, en agrandissant le groupe stabilisateur. Mais on peut le faire de plusieurs manières.

**Jauge**

On peut fragmenter les $d-1=2$ contraintes en $Z$ en les remplaçant (par exemple) par les $d(d-1)$ suivantes :

$$\hat Z_1=\begin{pmatrix}ZZ\bullet\\\bullet\bullet\bullet\\\bullet\bullet\bullet\end{pmatrix},\quad\begin{pmatrix}\bullet\bullet\bullet\\ZZ\bullet\\\bullet\bullet\bullet\end{pmatrix},\quad\hat Z_2=\begin{pmatrix}\bullet\bullet\bullet\\\bullet\bullet\bullet\\ZZ\bullet\end{pmatrix},\quad\hat Z_3=\begin{pmatrix}\bullet ZZ\\\bullet\bullet\bullet\\\bullet\bullet\bullet\end{pmatrix},\quad\begin{pmatrix}\bullet\bullet\bullet\\\bullet ZZ\\\bullet\bullet\bullet\end{pmatrix},\quad\hat Z_4=\begin{pmatrix}\bullet\bullet\bullet\\\bullet\bullet\bullet\\\bullet ZZ\end{pmatrix}.$$

Les $d^2-1=8$ contraintes indépendantes résultantes engendrent un groupe commutatif $\mathcal{S}_Z$, et définissent un sous-espace de dimension 2, codant 1 qubit. Cet espace est en fait le code de Shor, engendré par :

$$|\hat{\mathbf{0}}\rangle_Z=\frac{1}{2}\sum_{\substack{a+b+c\\\text{pair}}}\left|\begin{matrix}aaa\\bbb\\ccc\end{matrix}\right\rangle\qquad\text{et}\qquad|\hat{\mathbf{1}}\rangle_Z=\frac{1}{2}\sum_{\substack{a+b+c\\\text{impair}}}\left|\begin{matrix}aaa\\bbb\\ccc\end{matrix}\right\rangle.$$

On peut de la même façon fragmenter les contraintes en $X$ :

$$\hat X_1=\begin{pmatrix}X\bullet\bullet\\X\bullet\bullet\\\bullet\bullet\bullet\end{pmatrix},\quad\begin{pmatrix}\bullet X\bullet\\\bullet X\bullet\\\bullet\bullet\bullet\end{pmatrix},\quad\hat X_3=\begin{pmatrix}\bullet\bullet X\\\bullet\bullet X\\\bullet\bullet\bullet\end{pmatrix},\quad\hat X_2=\begin{pmatrix}\bullet\bullet\bullet\\X\bullet\bullet\\X\bullet\bullet\end{pmatrix},\quad\begin{pmatrix}\bullet\bullet\bullet\\\bullet X\bullet\\\bullet X\bullet\end{pmatrix},\quad\hat X_4=\begin{pmatrix}\bullet\bullet\bullet\\\bullet\bullet X\\\bullet\bullet X\end{pmatrix}$$

pour obtenir un autre groupe abélien $\mathcal{S}_X$ dont le sous-espace invariant est alors engendré par

$$|\hat{\mathbf{0}}\rangle_X=\frac{1}{8}\sum|\text{kets à colonnes de poids pairs}\rangle\quad\text{et}\quad|\hat{\mathbf{1}}\rangle_X=\frac{1}{8}\sum|\text{kets à colonnes de poids impairs}\rangle.$$

Le groupe de jauge $\mathcal{G}$ est le groupe engendré par $\mathcal{S}_X$ et $\mathcal{S}_Z$ (ou par $\mathcal{S}$ et les $\hat Z_i$ et $\hat X_i$). Le stabilisateur initial $\mathcal{S}$ est central dans $\mathcal{G}$, mais celui-ci n'est pas abélien (donc il ne laisse stable aucun vecteur non-nul).

On peut donc isoler un qubit logique en utilisant le stabilisateur $\mathcal{S}_Z$, ou bien $\mathcal{S}_X$ (ou encore un autre sous-groupe abélien de $\mathcal{G}$), mais ces différentes « jauges » ne stabilisent pas le même espace. Les valeurs logiques comme $|\hat{\mathbf{0}}\rangle$ et $|\hat{\mathbf{1}}\rangle$ sont représentées par des vecteurs qui dépendent de la jauge. Plus généralement la valeur logique $|q\rangle$ admet différentes représentations comme :

$$|\hat q\rangle_Z=|\hat q\rangle\otimes|0000\rangle_g\qquad\text{et}\qquad|\hat q\rangle_X=|\hat q\rangle\otimes|++++\rangle_g.$$

Par contre les opérateurs

$$\hat Z_L=\begin{pmatrix}ZZZ\\ZZZ\\ZZZ\end{pmatrix}\qquad\text{et}\qquad\hat X_L=\begin{pmatrix}XXX\\XXX\\XXX\end{pmatrix},$$

qui commutent avec $\mathcal{S}$ et anticommutent entre eux, définissent la valeur du qubit logique indépendamment de la jauge. Avec cette paire d'opérateurs, on peut observer que ce qubit protégé est exprimé par la parité globale (le syndrome pour l'opérateur $\hat Z_L$).

De la même façon, les paires $\{\hat Z_i,\hat X_i\}$ anticommutent et définissent les *qubits de jauge*. Le choix de la jauge revient à leur donner une valeur. Mais ces qubits de jauge sont en général perturbés par les mesures de syndrômes (associés aux fragments) et ne sont pas utilisés pour protéger de l'information quantique

Le centralisateur de $\mathcal{G}$ est engendré par $\mathcal{S}$, $\hat Z_L$ et $\hat X_L$. Les *bare logical operators* non-triviaux (qui opèrent uniquement sur le qubit protégé) sont les éléments de $\mathcal{C}(\mathcal{G})\setminus\mathcal{S}$. Ils sont donc représentés par $\hat Z_L$ et $\hat X_L$.

Le centralisateur de $\mathcal{S}$ est le groupe engendré par $\mathcal{G}$, $\hat{Z}_L$ et $\hat{X}_L$. Les *dressed logical operators* (qui peuvent opérer sur les qubits de jauge) non-triviaux (qui ont une action non-triviale sur le qubit protégé) sont les éléments de $\mathcal{C}(\mathcal{S}) \setminus \mathcal{G}$. Leur poids minimal est la distance du code. Ici c'est $d = 3$ : les opérateurs $\hat{Z}_L$ et $\hat{X}_L$ ont des représentants modulo $\mathcal{G}$ de poids $d$ (respectivement une colonne de $Z$, et une ligne de $X$).

Les dix opérateurs

$$\hat{Z}_i, \hat{X}_i \quad \text{pour } 1 \leqslant i \leqslant 4, \qquad \hat{Z}_L \text{ et } \hat{X}_L$$

forment un jeu de représentants du groupe $\mathcal{C}(\mathcal{S})/\mathcal{S}$, isomorphe au groupe de Pauli sur 5 qubits. Les huit premiers agissent sur les qubits de jauge (qui peuvent être représentés par les parités de $a_1+a_2$, $a_2+a_3$, $c_1+c_2$, $c_2+c_3$ dans (17)), et les deux derniers sur le qubit protégé (qui peut être représenté par la parité globale). D'autre part, les erreurs logiques associées au stabilisateur $\mathcal{S}$ peuvent être représentées par $\hat{Z}_i = S_{i-4}$ (pour $5 \leqslant i \leqslant 8$) et

$$\hat{X}_5 = \begin{pmatrix} Z\,Z\,\bullet \\ Z\,\bullet\,\bullet \\ Z\,\bullet\,\bullet \end{pmatrix}, \qquad \hat{X}_6 = \begin{pmatrix} \bullet\,\bullet\,Z \\ \bullet\,\bullet\,Z \\ \bullet\,Z\,Z \end{pmatrix}, \qquad \hat{X}_7 = \begin{pmatrix} \bullet\,\bullet\,\bullet \\ X\,\bullet\,\bullet \\ X\,X\,X \end{pmatrix}, \qquad \hat{X}_8 = \begin{pmatrix} X\,X\,X \\ \bullet\,\bullet\,X \\ \bullet\,\bullet\,\bullet \end{pmatrix}.$$

Inversement, on peut exprimer les $X_i$ et $Z_i$ physiques en fonction des logiques :

$$\begin{aligned}
X_1 &= \hat{X}_L\hat{X}_1\hat{Z}_5\hat{X}_7 & Z_1 &= \hat{Z}_L\hat{Z}_1\hat{X}_5\hat{Z}_8 \\
X_2 &= \hat{X}_L\hat{X}_1\hat{X}_3\hat{Z}_5\hat{X}_7\hat{X}_8 & Z_2 &= \hat{Z}_L\hat{X}_5\hat{Z}_8 \\
X_3 &= \hat{X}_L\hat{X}_3\hat{Z}_6\hat{X}_8 & Z_3 &= \hat{Z}_L\hat{Z}_3\hat{X}_5\hat{Z}_8 \\
X_4 &= \hat{X}_L\hat{Z}_5\hat{X}_7 & Z_4 &= \hat{Z}_L\hat{Z}_1\hat{Z}_2\hat{X}_5\hat{X}_6\hat{Z}_7 \\
X_5 &= \hat{X}_L\hat{X}_7\hat{X}_8 & Z_5 &= \hat{Z}_L\hat{X}_5\hat{X}_6 \\
X_6 &= \hat{X}_L\hat{Z}_6\hat{X}_8 & Z_6 &= \hat{Z}_L\hat{Z}_3\hat{Z}_4\hat{X}_5\hat{X}_6\hat{Z}_8 \\
X_7 &= \hat{X}_L\hat{X}_2\hat{Z}_5\hat{X}_7 & Z_7 &= \hat{Z}_L\hat{Z}_2\hat{X}_6\hat{Z}_7 \\
X_8 &= \hat{X}_L\hat{X}_2\hat{X}_4\hat{Z}_6\hat{X}_7\hat{X}_8 & Z_8 &= \hat{Z}_L\hat{X}_6\hat{Z}_7 \\
X_9 &= \hat{X}_L\hat{X}_4\hat{Z}_6\hat{X}_8 & Z_9 &= \hat{Z}_L\hat{Z}_4\hat{X}_6\hat{Z}_7
\end{aligned}$$

### Matrices de jauge

La présentation adoptée dans [27] des codes CSS à jauge correspond ici à :

$$H_X = \begin{pmatrix} 111111000 \\ 000111111 \end{pmatrix}, \qquad L_X = \begin{pmatrix} 100100000 \\ 001001000 \\ 000100100 \\ 000001001 \end{pmatrix}, \qquad H_Z = \begin{pmatrix} 110110110 \\ 011011011 \end{pmatrix}, \qquad L_Z = \begin{pmatrix} 110000000 \\ 011000000 \\ 000000110 \\ 000000011 \end{pmatrix}.$$

Les matrices $H_X$ et $H_Z$ décrivent le groupe stabilisateur $\mathcal{S}$. Les matrices $L_X$ et $L_Z$ décrivent les opérateurs logiques de jauge. On a

$$H_X H_Z^T = 0, \qquad L_X H_Z^T = 0, \qquad H_X L_Z^T = 0, \qquad L_X L_Z^T = I_k$$

où $k$ est le nombre de qubits de jauge.

### Décodage

Pour décoder le qubit protégé, on évalue les sous-syndromes correspondants aux fragments en $X$ et en $Z$ et on multiplie les issues pour obtenir les syndromes par les éléments de $S$. Pour corriger le qubit si on obtient, par exemple, les valeurs $(-1, +1)$ pour les deux derniers générateurs dans (16), on applique l'une des corrections équivalentes (parce que congrues modulo $\mathcal{G}$) suivantes :

$$\begin{pmatrix} X\,\bullet\,\bullet \\ \bullet\,\bullet\,\bullet \\ \bullet\,\bullet\,\bullet \end{pmatrix}, \qquad \begin{pmatrix} \bullet\,\bullet\,\bullet \\ X\,\bullet\,\bullet \\ \bullet\,\bullet\,\bullet \end{pmatrix}, \qquad \begin{pmatrix} \bullet\,\bullet\,\bullet \\ \bullet\,\bullet\,\bullet \\ X\,\bullet\,\bullet \end{pmatrix}, \qquad \begin{pmatrix} X\,\bullet\,\bullet \\ X\,\bullet\,\bullet \\ X\,\bullet\,\bullet \end{pmatrix}.$$

**Portes logiques transversales**

On remarque que la conjugaison par l'opérateur

$$\hat{H}'_L = \begin{pmatrix} HHH \\ HHH \\ HHH \end{pmatrix}$$

suivie d'une rotation d'un quart de tour du tableau des qubits physiques transforme les éléments de $\mathcal{S}_Z$ en éléments de $\mathcal{S}_X$, et réciproquement. Cette transformation échange aussi $\hat{Z}_L$ et $\hat{X}_L$. Cette transformation (rotation comprise) implémente donc une porte de Hadamard logique sur le qubit protégé.

Puisque le *phase-flip* logique $\hat{Z}_L$ est transversal, la porte CNOT est aussi transversale. Si le qubit logique de contrôle est $|\hat{\mathbf{0}}\rangle$ alors il est stable par $\hat{Z}_L$, donc somme de kets de poids pair. Mais l'opérateur $X^w$ avec $w$ de poids pair commute avec $\hat{Z}_L$ donc son action ne change pas le qubit protégé. Si le qubit de contrôle est $|\hat{\mathbf{1}}\rangle$ alors l'action sur le qubit protégé est celle de $X^w$ avec $w$ mots de poids impair. Ces $X^w$ anticommutent avec $\hat{Z}_L$ donc la valeur logique du qubit cible bascule.

## Le code de longueur 4

Le code sur 4 qubits (ici disposés en carré) stabilisé par les opérateurs

$$S_X = \begin{pmatrix} XX \\ XX \end{pmatrix} \qquad S_Y = \begin{pmatrix} YY \\ YY \end{pmatrix} \qquad S_Z = \begin{pmatrix} ZZ \\ ZZ \end{pmatrix}$$

est de dimension logique 2. Les opérateurs suivants

$$\hat{X}_1 = \begin{pmatrix} X\bullet \\ X\bullet \end{pmatrix} = \begin{pmatrix} \bullet X \\ \bullet X \end{pmatrix}, \qquad \hat{Z}_1 = \begin{pmatrix} ZZ \\ \bullet\bullet \end{pmatrix} = \begin{pmatrix} \bullet\bullet \\ ZZ \end{pmatrix}, \qquad \hat{X}_2 = \begin{pmatrix} XX \\ \bullet\bullet \end{pmatrix} = \begin{pmatrix} \bullet\bullet \\ XX \end{pmatrix}, \qquad \hat{Z}_2 = \begin{pmatrix} Z\bullet \\ Z\bullet \end{pmatrix} = \begin{pmatrix} \bullet Z \\ \bullet Z \end{pmatrix}$$

peuvent être choisis comme opérateurs logiques élémentaires puisqu'ils commutent avec les $S_i$ et entre eux, sauf $\hat{X}_i$ qui anticommute avec $\hat{Z}_i$ (pour $i = 1, 2$). On a alors

$$|\hat{0}\hat{0}\rangle = \frac{1}{\sqrt{2}}\left( \left|\begin{smallmatrix} 00 \\ 00 \end{smallmatrix}\right\rangle + \left|\begin{smallmatrix} 11 \\ 11 \end{smallmatrix}\right\rangle \right) \qquad |\hat{1}\hat{0}\rangle = \frac{1}{\sqrt{2}}\left( \left|\begin{smallmatrix} 01 \\ 01 \end{smallmatrix}\right\rangle + \left|\begin{smallmatrix} 10 \\ 10 \end{smallmatrix}\right\rangle \right)$$
$$|\hat{0}\hat{1}\rangle = \frac{1}{\sqrt{2}}\left( \left|\begin{smallmatrix} 00 \\ 11 \end{smallmatrix}\right\rangle + \left|\begin{smallmatrix} 11 \\ 00 \end{smallmatrix}\right\rangle \right) \qquad |\hat{1}\hat{1}\rangle = \frac{1}{\sqrt{2}}\left( \left|\begin{smallmatrix} 01 \\ 10 \end{smallmatrix}\right\rangle + \left|\begin{smallmatrix} 10 \\ 01 \end{smallmatrix}\right\rangle \right).$$

Autrement dit, le qubit logique de gauche est représenté par la parité des lignes, et celui de droite est représenté par la parité des colonnes.

Le groupe de jauge $\mathcal{G}$ formé de tous ces fragments a pour centralisateur $\mathcal{S} = \{I, S_X, S_Y, S_Z\}$. Chacun des deux qubits logiques peut-être considéré comme un qubit de jauge (mais un seul si on veut garder la possibilité d'encoder de l'information quantique).

Si on utilise la jauge constituée des fragments correspondant à $\hat{Z}_1$, alors le qubit de gauche est projeté (sur $|\hat{0}\rangle$ pour un résultat $++$, et à $|\hat{1}\rangle$ pour un résultat - -). Les stabilisateurs $S_X$ et $S_Z$ servent alors à détecter une erreur éventuelle sur le qubit restant (de droite). Les opérateurs sur ce qubit de droite sont $\hat{X}_2$ et $\hat{Z}_2$. La jauge constituée des fragments correspondant $\hat{X}_1$ projette aussi le qubit de gauche, mais sur $|\hat{+}\rangle$ ou $|\hat{-}\rangle$. Ces deux jauges peuvent être utilisées alternativement, sans altérer la valeur du qubit de droite.

Les jauges constituées des fragments correspondant à $\hat{X}_2$ ou à $\hat{Z}_2$ font le contraire.

Quelle que soit la jauge, les opérateurs

$$\hat{X}_1\hat{X}_2 = \begin{pmatrix} X\bullet \\ \bullet X \end{pmatrix} = \begin{pmatrix} \bullet X \\ X\bullet \end{pmatrix}, \qquad \hat{Y}_1\hat{Y}_2 = \begin{pmatrix} Y\bullet \\ \bullet Y \end{pmatrix} = \begin{pmatrix} \bullet Y \\ Y\bullet \end{pmatrix}, \qquad \hat{Z}_1\hat{Z}_2 = \begin{pmatrix} Z\bullet \\ \bullet Z \end{pmatrix} = \begin{pmatrix} \bullet Z \\ Z\bullet \end{pmatrix}$$

sont les $\hat{X}$, $\hat{Y}$ et $\hat{Z}$ sur le qubit restant.

### Le code de longueur 6

Intermédiaire entre le code parfait à 5 qubits et le code de Steane, on trouve ce code, explicité dans [34], qui protège un qubit accompagné d'un qubit de jauge. Le groupe $\mathcal{S}$ engendré par

$$-YIZXXY, \qquad ZXIIXZ, \qquad IZXXXX, \qquad ZZZIZI$$

définit un code stabilisateur, dont les deux qubits logiques peuvent être explicités par les opérateurs

$$\hat{X}_l = ZIXIXI, \qquad \hat{Z}_l = IZIIZZ, \qquad \text{et} \qquad \hat{X}_g = IIIXII, \qquad \hat{Z}_g = IIIZIZ.$$

Le deuxième qubit est mal protégé, puisque $\hat{X}_g$ et $\hat{Z}_g$ sont des opérateurs non-triviaux (pas dans $\mathcal{S}$) de poids $< 3$. En le considérant comme un qubit de jauge, on obtient un code de poids minimal 3, protégeant le premier qubit logique des erreurs de poids 1.

## 11. Les codes topologiques

### Les codes toriques

Ce sont des codes CSS définis à partir d'un graphe dessiné à la surface d'un tore, introduits par Kitaev

Les codes de Kitaev forment une famille (paramétrée par $d \in \mathbb{N}^*$) de codes définis à partir d'un graphe torique. Le graphe est celui qu'on peut dessiner sur un tore avec $d \times d$ mailles carrées. À chacune des $2d^2$ arêtes de ce graphe, on associe un qubit physique. Le code $K_d$ est défini en énumérant des générateurs de son stabilisateur $\mathcal{S}$. Pour chaque sommet du graphe, on considère un générateur formé de quatre portes $X$ appliquées aux arêtes adjacentes (*cocycle* élémentaire). Pour chaque maille élémentaire du graphe, on considère un générateur formé de quatre portes $Z$ appliquées aux arêtes composant la maille (*cycle* élémentaire). Par cette construction, les générateurs commutent deux-à-deux. Le stabilisateur est le groupe (abélien) engendré par ces deux familles. Les (co-)chaînes (fermées) sont les sommes (représentent les produits de générateurs) de co-cycles élémentairee. Les cochaînes sont en fait les chaînes du graphe dual.

Le code est de longueur $2d^2$ qubits, et les deux familles de générateurs sont chacune de rang $d^2 - 1$. Le code permet donc d'encoder deux qubits logiques.

Une erreur $Z^w$ donne lieu à un syndrome $s_X$ qui s'apparente à une liste de sommets. Pour corriger, il faut apparier les sommets de cette liste et déterminer $w'$ formant les chemins d'appariement. Si $w'$ est homotope à $w$ alors appliquer $Z^w$ corrige l'erreur. Par la méthode duale, on corrige aussi les erreurs $X^w$.

Il existe des cycles qui ne sont pas des chaînes, donc des erreurs de syndrome nul qui ont une action non-triviale sur les états du code. Pour le tore, le groupe $H_i = \{cycles\}/\{chaînes\}$ est isomorphe à $\mathbb{Z}^2$. Leur longueur minimale de tels cycles est $d$. La distance minimale du code torique est donc $d$.

Avec une numérotation convenable des qubits (par balayage horizontal des arêtes horizontales puis des arêtes verticales) les matrices de contrôle (8) s'écrivent

$$G_X = (A \mid B) \quad \text{et} \quad G_Z = (B^T \mid -A^T) \tag{18}$$

avec

$$A = I_d \otimes (I_d + X_d) \quad \text{et} \quad B = (I_d + X_d) \otimes I_d \tag{19}$$

qui sont donc des matrices de taille $d^2 \times d^2$.

#### Exemple du code $K_2$

Pour $d = 2$ avec une numérotation convenable des arêtes, on a (les deux matrices sont de rang 3) :

$$G_X = \begin{pmatrix} 1&1&0&0&1&1&0&0 \\ 1&1&0&0&0&0&1&1 \\ 0&0&1&1&1&1&0&0 \\ 0&0&1&1&0&0&1&1 \end{pmatrix} = \begin{pmatrix} \text{cc} \\ \text{c3} \\ \text{3c} \\ \text{33} \end{pmatrix} \quad \text{et} \quad G_Z = \begin{pmatrix} 1&0&1&0&1&0&1&0 \\ 1&0&1&0&0&1&0&1 \\ 0&1&0&1&1&0&1&0 \\ 0&1&0&1&0&1&0&1 \end{pmatrix} = \begin{pmatrix} \text{aa} \\ \text{a5} \\ \text{5a} \\ \text{55} \end{pmatrix}.$$

On a donc

$$C_X^\perp = \{00, 33, 3c, c3, cc, 0f, f0, ff\} \qquad \text{et} \qquad C_Z^\perp = \{00, 55, 5a, a5, aa, 0f, f0, ff\}.$$

De plus

$$C_X = C_X^\perp \cup (03 \oplus C_X^\perp) \cup (30 \oplus C_X^\perp) \cup (33 \oplus C_X^\perp) \quad \text{et} \quad C_Z = C_Z^\perp \cup (05 \oplus C_Z^\perp) \cup (50 \oplus C_Z^\perp) \cup (55 \oplus C_Z^\perp).$$

Le code $K_2$ est linéairement engendré par les 4 kets suivants (en notation hexadécimale) :

$$\begin{aligned}
|00\rangle_K &= \frac{1}{\sqrt{8}}\big(|00\rangle + |33\rangle + |3c\rangle + |c3\rangle + |cc\rangle + |0f\rangle + |f0\rangle + |ff\rangle\big)\\
|01\rangle_K &= \frac{1}{\sqrt{8}}\big(|05\rangle + |36\rangle + |39\rangle + |c6\rangle + |c9\rangle + |0a\rangle + |f5\rangle + |fa\rangle\big)\\
|10\rangle_K &= \frac{1}{\sqrt{8}}\big(|50\rangle + |63\rangle + |6c\rangle + |93\rangle + |9c\rangle + |5f\rangle + |a0\rangle + |af\rangle\big)\\
|11\rangle_K &= \frac{1}{\sqrt{8}}\big(|55\rangle + |66\rangle + |69\rangle + |96\rangle + |99\rangle + |5a\rangle + |a5\rangle + |aa\rangle\big)
\end{aligned}$$

Avec ces choix, les opérateurs logiques sont représentés physiquement selon la table :

| Logique | Physique |
|---|---|
| $X_1$ | $X_1X_3$ ou $X_2X_4$ |
| $X_2$ | $X_5X_7$ ou $X_6X_8$ |
| $Z_1$ | $Z_1Z_2$ ou $Z_3Z_4$ |
| $Z_2$ | $Z_5Z_6$ ou $Z_7Z_8$ |

**Table 1.** Correspondance opérateurs logiques / physiques

Cela justifie que la distance minimale du code $K_2$ est 2.

### Distance minimale

Les mots de $C_X$ sont ceux qui sont orthogonaux aux mots associés aux cocycles. Ce sont donc les (réunion de) boucles sur le tore. Modulo $C_Z^\perp$, qui est engendré par les mots associés aux mailles, on peut réduire chaque boucle à des enroulements sur le tore, de longueur multiple de $d$. Les kets de la forme (1) pour $y \in C_X \setminus C_Z^\perp$ ont donc tous un poids multiple de $d$, avec minimum $d$. Donc $d_X = d$. On a aussi $d_Z = d$ puisque le graphe à mailles carrées est isomorphe à son dual. En conclusion le code quantique $K_d$ est de paramètres $[[2d^2, 2, d]]$.

### Autres représentations

Si on place les sommets d'un nouveau réseau sur les arêtes du graphe de Kitaev, on obtient la représentation « échiquier » du code torique. Les cases de l'échiquier correspondent aux sommets et aux facettes du graphe initial et correspondent respectivement aux stabilisateurs élémentaires en $X$ et en $Z$. Le volume du réseau échiquier est la moitié du volume du réseau de Kitaev.

Si on double le quadrillage de Kitaev par celui du dual, les stabilisateurs en $X$, ceux en $Z$, les qubits horizontaux et ceux verticaux forment les sommets du nouveau réseau.

### Codes toriques optimaux

Les codes toriques sont généralisés dans [5]. Par exemple, avec le réseau du pas du cavalier engendré par $(2, 1)$ et $(-1, 2)$ qui est un sous-réseau du réseau carré canonique. En faisant le quotient, la maille obtenue contient 5 points à coordonnées entières, qui forment le graphe complet $K_5$ avec les arêtes du réseau canonique. Son

dual (dessiné sur le tore) est aussi $K_5$. En numérotant les 10 arêtes convenablement, on obtient les matrices de contrôle suivantes à partir des cocycles élémentaires (X) et des cycles élémentaires (Z) :

$$H_X = \begin{pmatrix} 1&1&0&0&0&\quad 0&0&1&1&0\\ 0&1&1&0&0&\quad 1&1&0&0&0\\ 0&0&1&1&0&\quad 0&0&0&1&1\\ 0&0&0&1&1&\quad 0&1&1&0&0\\ 1&0&0&0&1&\quad 1&0&0&0&1 \end{pmatrix} \quad \text{et} \quad H_Z = \begin{pmatrix} 0&0&1&0&1&\quad 0&1&0&0&1\\ 1&0&0&1&0&\quad 0&0&1&0&1\\ 0&1&0&0&1&\quad 1&0&1&0&0\\ 1&0&1&0&0&\quad 1&0&0&1&0\\ 0&1&0&1&0&\quad 0&1&0&1&0 \end{pmatrix}.$$

Elles définissent un code quantique de longueur 10, encodant 2 qubits (les deux matrices de contrôle sont de rang 4), et de distance minimale 3 (selon l'argument de Kitaev, le tore initial étant de taille 3x3). On retrouve ici (en réordonnant les qubits) le code CSS $[[10, 2, 3]]$ (15) associé au code à 5 qubits.

Plus généralement, on peut prendre le réseau engendré par $(r, s)$ et $(-s, r)$, et poser $d = r + s$ (c'est la longueur du chemin en escalier joignant deux points du réseau, voisins). Le nombre de points du tore quotient est le volume $r^2 + s^2$ et ils sont reliés par $n = 2(r^2 + s^2)$ arêtes du réseau carré. Chaque sommet définit une contrainte en $X$ via son cocycle. La somme de ces contraintes est triviale, il reste $n/2 - 1$ contraintes en $X$ et, de façon analogue en $Z$. On obtient un code $(n, 2, d)$.

De plus, on a $n - d^2 = (s - r)^2$. L'article [5] considère le cas optimisé $s = r + 1$, qui procure des codes de type $[[d^2 + 1, 2, d]]$.

**Version quadridimensionnelle**

Le réseau hypercubique quadridimensionnel périodique de taille $d$ possède $d^4$ sommets, $4d^4$ arêtes élémentaires, $6d^4$ carrés élémentaires, et $4d^4$ cubes élémentaires.

Les qubits sont placés sur les carrés élémentaires, les $X$-générateurs sont les arêtes élémentaires (entourées de 6 qubits), les $Z$-générateurs sont les cubes élémentaires (de poids 6 qubits aussi). Les $Z$-opérateurs logiques sont représentés par des surfaces sans bord et les $X$-opérateurs logiques idem mais dans le réseau dual. Le code torique obtenu est donc de paramètres $[[6d^4, 6, d^2]]$.

## Codes biblocs

Ce sont les codes CSS obtenus (sur un corps fini quelconque $\mathbb{F}_q$) en prenant deux matrices de contrôle sous la forme (18) avec deux matrices carrées $A$ et $B$ qui commutent (afin de réaliser la condition d'orthogonalité $G_X G_Z^\perp = 0$).

**Codes bicycles**

On peut garantir la commutativité en choisissant pour $A$ et $B$ des matrices circulantes de taille $\ell \times \ell$. On parle alors de codes bicycles généralisés (le cas bicycle simple correspond en plus à $B = A^T$). Dans ce cas circulant, la transposition peut s'exprimer comme une permutation de lignes puis de colonnes. Il en résulte que $\mathsf{rg}(A|B) = \mathsf{rg}(B^T|A^T)$, ce qui simplifie l'expression de la q-dimension du code : c'est $2\big(\ell - \mathsf{rg}(A \mid B)\big)$. On peut aussi écrire $A = a(\Delta_\ell)$ et $B = b(\Delta_\ell)$ où $\Delta_\ell$ est la matrice de permutation cyclique $i \mapsto i + 1$ modulo $\ell$ avec deux polynômes $a, b \in \mathbb{F}_q[X]$ de degré $< \ell$.

**11.1. — Proposition [31][42].** *Posons $h = \mathsf{pgcd}(a, b, X^\ell - 1)$. On a $\mathsf{rg}(A|B) = \ell - \deg h$.*

Démonstration — L'espace engendré par les colonnes de $(A|B)$ s'identifie à l'ensemble des

$$ua + vb \bmod (X^\ell - 1) \qquad \text{avec } u, v \in \mathbb{F}_q[X] \text{ de degrés } < \ell. \tag{20}$$

Par Bézout, il existe $u_0, v_0, w_0 \in \mathbb{F}_q[X]$ tels que $u_0 a + v_0 b + w_0(X^\ell - 1) = h$. Pour $0 \leqslant m < \ell - \deg h$, les combinaisons (20) obtenues avec $u = X^m u_0$, $v = X^m v_0$ donnent des valeurs $X^m h$ linéairement indépendantes. Donc $\mathsf{rg}(A|B) \geqslant \ell - \deg h$. Mais dans (20) chaque terme est multiple de $h$ donc cette borne n'est pas dépassée. □

**11.2. — Corollaire.** *La q-dimension du code bicycle est* $2\,\deg h$. □

Aussi, la distance minimale est minorée par celle du code classique sur $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ contrôlé par $\alpha A + B$, comme évoqué dans [24]. D'après le théorème 3.2, la distance minimale est donnée par

$$d = \mathsf{min}\{\mathsf{wt}(w) \in \mathsf{ker}(A \mid B) \setminus \mathrm{rs}(B^T \mid A^T)\}$$

où $\mathrm{rs}(\cdot)$ désigne le sous-espace engendré par les lignes de la matrice. (On a $d_Z = d_X$.)

**Codes 2BGA**

On peut plus généralement garantir la commutativité en prenant $a$ et $b$ dans une l'algèbre de groupe $\mathbb{F}_q[G]$ où $G$ est un groupe fini d'ordre $\ell$ et en posant

$$A = L(a) = \sum_{g\in G} a_g \Delta_g \qquad \text{et} \qquad B^T = R(b) = \sum_{g\in G} b_g \Delta'_g$$

où $\Delta_g$ et $\Delta'_g$ sont respectivement la matrice de permutation $i \mapsto gi$ et celle de $i \mapsto ig$ [27]. Autrement dit, $A$ et $B^T$ sont les matrices $\ell \times \ell$ à coefficients dans $G$ de l'action de $a$ à gauche et de $b$ à droite exprimées dans la base canonique de $\mathbb{F}_q[G]$. (Si $P$ est la matrice de l'application $\sum_g a_g g \mapsto \sum_g a_g g^{-1}$ on a $R(b)^T = PL(b)P$.)

On peut alternativement décrire les codes 2BGA comme étant les codes $\mathsf{CSS}(C_1, C_2)$ avec

$$C_1 = \big\{(u, v) \in \mathbb{F}_q[G] \;\big|\; au = vb\big\} \qquad \text{et} \qquad C_2 = \big\{(wb \mid aw) \;\big|\; w \in \mathbb{F}_q[G]\big\}.$$

Comme cas particulier des codes 2BGA on a le cas quasi-cyclique où $A$ et $B$ sont des matrices semi-circulantes :

$$A = I_m \otimes R \qquad \text{et} \qquad B = R \otimes I_m$$

où $R$ est une somme de puissances de $\Delta_\ell$. (L'index $m$ est le nombre de cycles, et $\ell$ est leur longueur.) Cela définit des codes de longueur $2m\ell$. On retrouve en particulier le code de Kitaev (en ordonnant convenablement les qubits) qui correspond au cas où $R = I + \Delta_\ell$ est une matrice de contrôle du code à répétition (des 1 sur la diagonale et la sous-diagonale).

**Codes HGP (produit d'hypergraphes)**

Ils reprennent une structure proche de (18) mais avec

$$G_X = (A \mid B) \qquad \text{et} \qquad G_Z = (B' \mid -A') \tag{21}$$

où

$$A = I_{m_1} \otimes H_2, \qquad B = H_1 \otimes I_{m_2}, \qquad A' = I_{n_1} \otimes H_2^T, \qquad B' = H_1^T \otimes I_{n_2}$$

où les matrices $H_i$ de tailles $m_i \times n_i$ sont les matrices de contrôle de codes $C_i$ de dimension $k_i$ et de distances minimales $d_i$. On a donc $A$, $B$, $A'$ et $B'$ de tailles respectives $m_1m_2 \times m_1n_2$, $m_1m_2 \times n_1m_2$, $n_1n_2 \times n_1m_2$, et $n_1n_2 \times m_1n_2$. On a bien la condition d'orthogonalité :

$$AB'^T - BA'^T = 0. \tag{22}$$

On notera $\tilde{k}_i$ et $\tilde{d}_i$ les dimensions et distances minimales des codes contrôlés par $H_i^T$ (donc $\tilde{k}_i = k_i + r_i - n_i$). On a alors [25] :

**11.3. — Proposition.** $\mathsf{rg}(A \mid B) = m_1m_2 - \tilde{k}_1\tilde{k}_2$ *et* $\mathsf{rg}(B' \mid A') = n_1n_2 - k_1k_2$.

Démonstration — On voit que $(u \mid v)(A \mid B) = 0$ (noyau à gauche) si et seulement si $uH_1 = 0$ et $vH_2 = 0$, c'est-à-dire $u \in C_1^T$ et $v \in C_2^T$. On a donc $\tilde{k}_1\tilde{k}_2$ choix de $(u, v)$ qui définissent des dépendances dans les lignes de $(A \mid B)$. □

**11.4. — Proposition.** *Le code obtenu a pour paramètres* $[[N, K, D]]$ *avec*

$$N = m_1n_2 + n_1m_2, \qquad K = 2k_1k_2 - k_1(n_2 - m_2) - k_2(n_1 - m_1) = k_1\tilde{k}_2 + \tilde{k}_1k_2, \qquad D \geqslant \mathsf{min}(d_1, d_2, \tilde{d}_1, \tilde{d}_2).$$

**11.5. — Cas particuliers.** (a) (Tillich-Zémor). Prendre $H_1$ une matrice $(n-k) \times n$ de rang maximal, et $H_2 = H_1^T$. On a $m_1 = n_2 = n$, $n_1 = m_2 = n - k$, $\tilde{k}_1 = k_2 = k$, $k_1 = \tilde{k}_2 = 0$. Donc $N = n^2 + (n-k)^2$ et $K = k^2$.

(b) Pour $H_i$ de taille $n_i \times n_i$ définissant des codes $[n_i, k_i, d_i]$, on a $\tilde{k}_i = k_i$ donc $N = 2n_1n_2$ et $K = 2k_1k_2$.

(c) On retrouve le code de Kitaev avec les matrices (19) pour lesquelles $m_i = n_i = d$, $k_i = 1$, $N = 2d^2$ et $K = 2$.

**Construction de Tillich–Zémor**

On part de deux codes classiques $\mathcal{C}_i$ (pour $i = 1, 2$) donnés par leurs graphes de Tanner $G_i = (V_i, C_i, E_i)$. En intervertissant $V_i$ avec $C_i$, on obtient un code noté $\mathcal{C}_i^T$ dit *transposé* de $\mathcal{C}_i$ (car cela revient à transposer une matrice de contrôle). Par invariance du rang par transposition on a

$$|V_i| - \mathsf{dim}\, \mathcal{C}_i = |C_i| - \mathsf{dim}\, \mathcal{C}_i^T.$$

On pose alors

$$V = V_1 \times V_2 \cup C_1 \times C_2 \quad \text{et} \quad C = C_X \cup C_Z \qquad \text{avec} \qquad C_X = C_1 \times V_2 \quad \text{et} \quad C_Z = V_1 \times C_2.$$

Soit $E_X$ l'ensemble des arêtes qui relient chaque $(c_1, v_2) \in C_X$ à chaque $(c_1, c_2)$, pour $c_2 \in C_2$, et à chaque $(v_1, v_2)$, pour $v_1 \in C_1$. De façon similaire, les arêtes de $E_Z$ relient chaque $(v_1, c_2) \in C_X$ à chaque $(c_1, c_2)$, pour $c_1 \in C_1$, et à chaque $(v_1, v_2)$, pour $v_2 \in C_2$. Les graphes $G_X = (V, C_X, E_X)$ et $G_Z = (V, C_Z, E_Z)$ peuvent être interprétés comme les graphes de Tanner de deux codes $\mathcal{C}_X$ et $\mathcal{C}_Z$. Le code quantique construit par Tillich & Zémor est alors $\mathsf{CSS}(\mathcal{C}_X, \mathcal{C}_Z)$.

**Formulation de Panteleev**

En s'appuyant sur des correspondances du type ($H$ est une matrice $m \times n$ et chaque $v_i$ est dans $\mathbb{F}_2^m$)

$$(v_1, \ldots, v_r) \cdot (I_r \otimes H) = (v_1 H, \ldots v_r H) \longleftrightarrow \begin{pmatrix} v_1 H \\ \vdots \\ v_r H \end{pmatrix} = \begin{pmatrix} v_1 \\ \vdots \\ v_r \end{pmatrix} H$$

Pavel Panteleev redéfinit les codes HGP en exprimant les codes $C_1$ et $C_2$ de la construction CSS sous la forme suivante :

$$C_1 = \left\{ (U \mid V) \in \mathbb{F}_2^{n_a \times n_b + m_a \times m_b} \;\middle|\; AU = VB \right\} \qquad \text{et} \qquad C_2 = \left\{ (WB \mid AW) \;\middle|\; W \in \mathbb{F}_2^{n_a \times m_b} \right\}$$

où $A$ et $B$ sont des matrices $m_a \times n_a$ et $m_b \times n_b$. Pour $A = B = H$ de taille $m \times n$ et de rang $m$, on retrouve les codes $[[n^2 + m^2, (n-m)^2]]$ de Tillich-Zémor (la condition $(I \otimes H)u + (H^T \otimes I)v = 0$ devient $(I \otimes H)u + (v^T (H \otimes I))^T = 0$ puis $HU + V^T H = 0$).

**Codes LP (*lifted product*)**

Il reprennent la structure (21) mais où $A$ et $B$ sont des matrices $m \times n$ de blocs $\ell \times \ell$ (ou à coefficients dans une algèbre, module libre de rang $\ell$) [32].

- Pour $\ell = 1$ on retrouve les codes HGP.
- Pour $m = n = 1$ ce sont les codes bicycles généralisés.
- Lorsque le module est une algèbre de groupe (avec un groupe d'ordre $\ell$) ce sont les codes 2BGA.

## Homologie

Soit $G$ un graphe connexe dessiné sur une variété $M$ (sans croisements). Soient $V$, $E$, $F$ ses ensembles de sommets, d'arêtes, et de régions. La caractéristique d'Euler de $G$ est donnée par

$$\chi(G) = |V| - |E| + |F|.$$

Dans le cas d'un graphe planaire, $\chi(G)$ est égal à 2, et peut descendre à $2(1-g)$ sur une surface orientée de genre $g$.

On note $C_i$ (avec $i = 0, 1, 2$) les $\mathbb{F}_2$-espaces vectoriels de bases respectives $V$, $E$ et $F$. Les éléments de $C_i$ sont appelés des $i$-chaînes. On a les opérateurs bords $\partial_1$ et $\partial_2$ :

$$\{0\} \xrightarrow{\partial_3} C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\partial_0} \{0\} \tag{23}$$

qui sont les opérateurs linéaires tels que $\partial_1$ d'une arête est la somme de ses deux extrémités, et $\partial_2$ d'une région est la somme des arêtes qui forment sa frontière. On a en particulier $\partial_1 \circ \partial_2 = 0$. On note $Z_i = \ker \partial_i$ et $B_i = \operatorname{im} \partial_{i+1}$. On a $B_i \subseteq Z_i$. La matrice de $\partial_1$ dans une base « canonique » est une matrice d'incidence de $G$.

Pour chaque $i$, on note $C^i$ le dual de $C_i$ (l'espace des formes linéaires $C_i \to \mathbb{F}_2$). On a les applications transposées $\partial^i = \partial_i^T : C^{i+1} \to C^i$ :

$$\{0\} \xleftarrow{\partial^3} C^2 \xleftarrow{\partial^2} C^1 \xleftarrow{\partial^1} C^0 \xleftarrow{\partial^0} \{0\}.$$

Ils s'identifient en fait aux opérateurs cobords (les opérateurs bords du graphe dual) puisque les matrices d'adjacence du graphe dual sont les transposées de celles du graphe primal. Par exemple, pour $v \in V$, notons $v^*$ l'élément de $C^0$ tel que $v^*(v) = 1$ et $v^*(w) = 0$ pour $w \neq v$. La forme $\partial^1(v^*) = v^* \circ \partial_1 \in C^1$ est celle qui associe 1 à un chemin $e \in C_1$ si et seulement si $v$ est extrémité (simple) de $e$. On a $\partial^2 \circ \partial^1 = 0$. Je note $Z^i = \ker \partial^{i+1}$ et $B^i = \operatorname{im} \partial^i$. On a $B^i \subseteq Z^i$.

**11.6. — Propriété.** *Soit $f : U \to V$ une application linéaire. On a*

$$\operatorname{im}(f^T) = (\ker f)^\perp \qquad \textit{et} \qquad \ker(f^T) = (\operatorname{im} f)^\perp.$$

Démonstration — Il suffit de démontrer la deuxième égalité. Pour $\alpha \in V^*$, on a $f^T(\alpha) = 0$ ssi $\alpha \circ f = 0$ ssi $\alpha \perp \operatorname{im} f$. □

En particulier, $\operatorname{im} \partial^1 = (\ker \partial_1)^\perp \subseteq (\operatorname{im} \partial_2)^\perp$ donc

$$B_1 = \operatorname{im} \partial_2 \perp \operatorname{im} \partial^1 = B^1. \tag{24}$$

Concrètement, un chemin est sans extrémité simple si et seulement si son image est nulle par tout $\partial^1(v^*)$.

Les groupes d'homologie et de cohomologie (avec $i = 0, 1, 2$) sont respectivement les quotients

$$H_i = \frac{Z_i}{B_i} = \frac{\ker \partial_i}{\operatorname{im} \partial_{i+1}} \qquad \text{et} \qquad H^i = \frac{Z^i}{B^i} = \frac{\ker \partial^{i+1}}{\operatorname{im} \partial^i}.$$

Puisque les espaces $C_i$ et $C^i$ ont même dimension et les applications $\partial_i$ et $\partial^i$ ont même rang, les espaces $H_i$ et $H^i$ ont tous deux même dimension $\dim C_i - \operatorname{rg} \partial_i - \operatorname{rg} \partial_{i+1}$.

**11.7. — Proposition.** *La caractéristique d'Euler de $G$ est*

$$\chi(G) = \dim H_0 - \dim H_1 + \dim H_2.$$

Démonstration — Parce que

$$\begin{aligned}
\chi(G) &= \dim C_0 - \dim C_1 + \dim C_2 \\
&= (\dim \operatorname{im} \partial_0 + \dim \ker \partial_0) - (\dim \operatorname{im} \partial_1 + \dim \ker \partial_1) + (\dim \operatorname{im} \partial_2 + \dim \ker \partial_2) \\
&= 0 + \dim(\ker \partial_0 / \operatorname{im} \partial_1) - \dim(\ker \partial_1 / \operatorname{im} \partial_2) + \dim(\ker \partial_2 / \{0\}) \\
&= \dim H_0 - \dim H_1 + \dim H_2.
\end{aligned}$$

□

En particulier, pour une surface orientée de genre $g$ (tore à $g$ trous) on retrouve $\chi(G) = 1 - 2g + 1 = 2(1-g)$.

**Interprétation homologique des codes CSS**

Tout code CSS est défini par deux matrices $H_X$ et $H_Z$ de tailles respectives $m_X \times n$ et $m_Z \times n$ telles que $H_X H_Z^T = 0$. On supposant que les rangs de $H_X$ et $H_Z$ soient $m_X$ et $m_Z$, on obtient une chaîne

$$\mathbb{F}_q^{m_Z} \xrightarrow{H_Z^T} \mathbb{F}_q^n \xrightarrow{H_X} \mathbb{F}_q^{m_X}.$$

Réciproquement, à partir d'une chaîne homologique de type (23) nous pourrons construire un code CSS en utilisant $\partial_1$ et $\partial_2^T$ pour définir les matrices $H_X$ et $H_Z$. La dimension du code obtenu est

$$n - m_X - m_Z = \dim \ker \partial_1 - \dim \operatorname{im} \partial_2 = \dim H_1.$$

La distance minimale est donnée par $\min(d_X, d_Z)$ où

$$d_X = \text{poids minimal dans } \ker \partial_1 \setminus \operatorname{im} \partial_2, \qquad \text{et} \qquad d_Z = \text{poids minimal dans } \ker \partial^2 \setminus \operatorname{im} \partial^1.$$

### Codes homologiques

On associe un qubit physique à chaque élément de $E$. Les éléments de $C_1$ s'identifient alors aux kets de la base canonique de $\mathbb{C}^n$ avec $n = |E|$. Le groupe des stabilisateurs en $Z$ est formé des opérateurs en $Z$ de support dans $B_1 = \mathsf{im}\,\partial_2$. Celui des stabilisateurs en $X$ est formé des opérateurs en $X$ dont le support est dans $B^1 = \mathsf{im}\,\partial^1$. D'après (24) ces deux ensembles de supports sont orthogonaux (donc tous les stabilisateurs commutent). On obtient un code de longueur $n$ et de q-dimension $k = \mathsf{dim}\,C_1 - \mathsf{rg}\,\partial_2 - \mathsf{rg}\,\partial_1 = \mathsf{dim}\,H_1$, dont une base est donnée par les

$$|\overline{c}\rangle := \frac{1}{|B^1|}\sum_{b\in B^1}|c+b\rangle \qquad \text{pour } \overline{c}\in H^1$$

qui, par construction, sont stables par les opérateurs en $X$ de support dans $B^1$ et ceux en $Z$ de support dans $B_1$.

Les couples (chemin fermé, cochemin fermé)$\in Z_1\times Z^1$ s'identifient (en ignorant les phases globales) au normalisateur $\mathcal{N}(\mathcal{S})$ par $(c,c^*)\mapsto Z^cX^{c^*}$. Les éléments non-triviaux de $H_1$ (respectivement de $H^1$) sont des bords dont les $Z$-opérateurs (respectivement $X$-opérateurs) associés ont une action non-triviale sur le code. On obtient ainsi les $2k$ opérateurs logiques de Pauli $\in \mathcal{N}(\mathcal{S})/\mathcal{S}$. Les chemins ou cochemins non homologues à zéro de longueur minimale définissent la distance minimale du code.

Une erreur $e$ de type $Z$ est un élément de $C_1$. Son syndrome s'identifie à $\partial_1(e)\in C_0$. Pour corriger cette erreur, on applique un $Z$-opérateur associé à un élément $C_1$ ayant même $\partial_1$ que $e$. Si les deux sont homologues (congrus modulo $\mathsf{im}\,\partial_2$) la correction n'affecte pas les qubits logiques. Références : [3][5][8].

### Produit tensoriel de chaînes homologiques

Une chaîne homologique générale $\mathcal{C}$ s'écrit

$$\cdots \xrightarrow{\partial_{i+2}} C_{i+1} \xrightarrow{\partial_{i+1}} C_i \xrightarrow{\partial_i} C_{i-1} \xrightarrow{\partial_{i-1}} \cdots$$

ou encore $C=\bigoplus_i C_i$ avec $\partial : C\to C$ telle que $\partial(C_i)\subseteq C_{i-1}$ pour tout $i$. Un élément de $C_i$ est dit élément de degré $i$.

Pour $\mathcal{A}$ et $\mathcal{B}$ deux chaînes sur $\mathbb{F}_2$, on peut définir leur produit tensoriel $\mathcal{C}=\mathcal{A}\otimes\mathcal{B}$ en posant

$$C = A\otimes B = \bigoplus_k C_k \qquad \text{avec} \qquad C_k = \bigoplus_{i+j=k} A_i\otimes B_j$$

et en définissant $\partial$ sur $A\otimes B$ par $\partial(a\otimes b)=\partial a\otimes b + a\otimes \partial b$.

Le code de Kitaev entre dans ce cadre

$$\mathbb{F}_2^\ell\times F_2^\ell \xrightarrow{\partial_2} F_2^\ell\times F_2^\ell \oplus F_2^\ell\times F_2^\ell \xrightarrow{\partial_1} \mathbb{F}_2^\ell\times F_2^\ell$$

où les deux termes de l'espace central correspondent aux qubits (arêtes) horizontales et verticales respectivement et

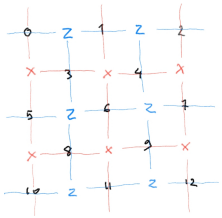
$$\partial_1 = I\otimes(1+X)+(1+X)\otimes I \qquad \text{et} \qquad \partial_5 = (1+X)\otimes I + I\otimes(1+X).$$

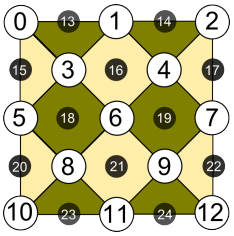
## Codes surface

### Codes planaires

Pour n'importe quel graphe $G=(V,E,F)$ connexe planaire (sur le plan ou une sphère) on a $\chi(G) = |V|-|E|+|F| = 2$. En associant un qubit à chaque arête, un stabilisateur en $X$ à chaque sommet et un stabilisateur en $Z$ à chaque région on obtient $|V|+|F|-2=|E|$ stabilisateurs indépendants (la somme de ceux en $X$ est triviale, ainsi que la somme de ceux en $Z$). On obtient donc un code à 0 qubits (qui stabilise un unique état quantique). On peut obtenir un nombre de qubits logiques $>0$ en introduisant des « trous », c'est-à-dire en retirant des stabilisateurs associés à des sommets ou à des régions, ou bien en introduisant des bords.

Par exemple, avec un réseau carré de $d \times d$ arêtes horizontales et $(d-1) \times (d-1)$ arêtes verticales, on obtient un code $[[d^2 + (d-1)^2, 1, d]]$ où les deux opérateurs logiques sont représentés par un chemin reliant deux bords opposés. Pour $d = 3$ c'est le code surface-25, de type $[[13, 1, 3]]$ qu'on trouve plus souvent schématisé par cette figure (à droite) :






où les 13 qubits physiques sont les sommets blancs (ce sont les arêtes d'un graphe qui relierait les régions claires). Les sommets noirs sont des qubits auxiliaires utilisés pour mesurer les syndromes en $X$ (régions claires) ou en $Z$ (régions sombres).

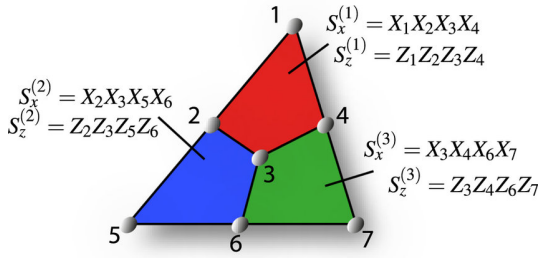
Pour ces codes, la distance minimale $d$ est apparentée à une longueur (celle de chemins d'homotopie non-triviale) et la longueur $n$ est apparentée à une aire. Cela limite $d$ à $O(\sqrt{n})$. Comme le nombre $k$ de qubits logiques est lié aux nombre de défauts, on a même $kd^2 = O(n)$.

### Codes couleurs

Voir [4]. Les codes couleurs 2D sont basés sur des graphes $(V, E, F)$ de degré 3 et dont le dual est 3-colorable (appelés 2-colexes). Cela implique qu'on peut attribuer aussi aux arêtes une couleur (celle différente des faces séparées par l'arête). Les sommets désignent des qubits et chaque facette est associée à deux opérateurs stabilisateurs, un en $X$ et un en $Z$, ayant pour support les sommets de la facette. Il y a $2|F|-4$ stabilisateurs (facette) indépendants.

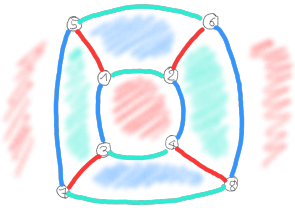
À chaque couleur $c$, on peut associer un sous-réseau dont les arêtes sont celles de couleur $c$ et dont les sommets correspondent aux facettes de couleur $c$ du réseau initial.

Pour chaque classe d'homotopie on peut suivre un lacet de cette classe pour chacune des trois couleurs. Le produit de deux de ces lacets donne celui de l'autre couleur ; il y a donc deux lacets indépendants par classe. Pour chacun d'eux on peut faire un opérateur en $X$ et un autre en $Z$. On obtient ainsi $8g$ opérateurs logiques (où $g$ est le genre du graphe) qui définissent un code à $4g$ qubits.




### Le code cubique [[8,3,2]]

C'est un code couleurs 3D. Il est basé sur le graphe cubique (8 sommets, 12 arêtes, 6 facettes) :



dont les sommets sont associés à des qubits physiques. Il est stabilisé par :

$$ZZZZIIII \text{ (facette rouge)}, \quad ZZIIZZII \text{ (facette bleue)}, \quad ZIZIZIZI \text{ (facette verte)},$$
$$ZZZZZZZZ, \quad XXXXXXXX \text{ (autres facettes)}.$$

Les opérateurs logiques sont :

$$\hat{X}_1 = XXXXIIII, \quad \hat{X}_2 = XXIIXXII, \quad \hat{X}_3 = XIXIXIXI,$$
$$\hat{Z}_1 = ZIIIZIII, \quad \hat{Z}_2 = ZIZIIIII, \quad \hat{Z}_3 = ZZIIIIII$$

de telle sorte que les états de la base logique sont :

$$\widehat{|000\rangle} = \frac{1}{\sqrt{2}}\big(|00000000\rangle + |11111111\rangle\big), \quad \widehat{|111\rangle} = \frac{1}{\sqrt{2}}\big(|10010110\rangle + |01101001\rangle\big),$$
$$\widehat{|100\rangle} = \frac{1}{\sqrt{2}}\big(|11110000\rangle + |00001111\rangle\big), \quad \widehat{|011\rangle} = \frac{1}{\sqrt{2}}\big(|01100110\rangle + |10011001\rangle\big),$$
$$\widehat{|010\rangle} = \frac{1}{\sqrt{2}}\big(|11001100\rangle + |00110011\rangle\big), \quad \widehat{|101\rangle} = \frac{1}{\sqrt{2}}\big(|01011010\rangle + |10100101\rangle\big),$$
$$\widehat{|001\rangle} = \frac{1}{\sqrt{2}}\big(|10101010\rangle + |01010101\rangle\big), \quad \widehat{|110\rangle} = \frac{1}{\sqrt{2}}\big(|00111100\rangle + |11000011\rangle\big).$$

Les portes de Hadamard sont transversales :

$$\hat{H}_1 = HHHHIIII, \quad \hat{H}_2 = HHIIHHII, \quad \hat{H}_3 = HIHIHIHI.$$

La porte transversale

$$TT^\dagger T^\dagger TT^\dagger TTT^\dagger$$

implémente la porte triple CCZ (qui n'est pas dans le groupe de Clifford) sur les trois qubits logiques.

**Bornes topologiques**

On considère des codes stabilisateurs dont les qubits sont placés aux sommets d'un réseau $D$-dimensionnel $\Lambda = \{1, \cdots, L\}^D$ (avec une topologie à bord ou torique). On a des bornes supérieures sur la distance minimale sous la condition de localité :

Les supports des générateurs du stabilisateur sont contenus dans des $D$-hypercubes de côté $r$. (25)

**11.8. — Lemme (de nettoyage) [7].** *Soit $M \subseteq \Lambda$. Alors l'une de deux assertions suivante est vraie :*
*(a) L'un des opérateurs logiques $\mathcal{P} \in \mathcal{C}(\mathcal{S}) \setminus \mathcal{S}$ a son support inclus dans $M$.*
*(b) Tout opérateur logique $\mathcal{P} \in \mathcal{C}(\mathcal{S})$ admet un représentant modulo $\mathcal{S}$ dont le support évite $M$.*

**11.9. — Définition.** On dit qu'un ensemble $M$ de qubits d'un code donné est un *ensemble corrigible* si on peut encore reconstruire l'état encodé malgré la perte des qubits de $M$.

Le lemme de nettoyage implique que pour tout ensemble corrigible $M$, les opérateurs logiques non-triviaux ont des représentants évitant $M$.

**11.10. — Proposition [7].** *Sous la condition de localité (25), avec en plus $L \geqslant (r-1)^2$, l'un des opérateurs logiques $\mathcal{P} \in \mathcal{C}(\mathcal{S})$ a son support contenu dans une tranche de $\Lambda$ d'épaisseur $r$.*

Démonstration — On suppose au contraire que tous les opérateurs logiques ont une épaisseur $> r$. On divise $\Lambda$ en un nombre pair de tranches d'épaisseur $r-1$ et/ou $r$ (c'est possible dès que $L \geqslant 2(r-1)^2$). Par l'hypothèse et d'après 11.8, on peut chasser chaque opérateur logique de n'importe quelle tranche. On peut même le chasser simultanément de toutes les tranches paires, grâce à la condition (25). L'opérateur obtenu a donc son support contenu dans les tranches impaires. Toujours d'après (25), il est produit d'opérateurs

individuellement contenus dans une seule tranche impaire. Ces facteurs sont aussi nécessairement dans $\mathcal{C}(\mathcal{S})$, ce qui contredit l'hypothèse. □

Sous la condition (25) la proposition ci-dessus montre que le support d'un opérateur logique est contenu dans une structure quasiment $D-1$-dimensionnelle (une tranche d'épaisseur $r$) donc de cardinal $O(L^{D-1})$. Comme le réseau est $D$-dimensionnel, la longueur du code est en $\Theta(L^D)$. On obtient la borne [7] :

$$d \in O(n^{1-1/D}). \tag{26}$$

Sous la même condition de localité on a aussi [6] :

$$kd^{2/(D-1)} \in O(n) \tag{27}$$

pour un code de q-dimension $k$. Enfin, on a la borne de Haah (sous une condition d'homogénéité) [18] :

$$k \in O(n^{1-2/D}). \tag{28}$$

Pour $D = 2$, la borne (27) implique la borne (26), et elles sont toutes les deux atteintes par le code torique.

**11.11. — Théorème (du séparateur planaire).** *Soit $G$ un graphe planaire à $n$ sommets. Alors il existe une partition $A \sqcup T \sqcup B$ de l'ensemble des sommets de $G$ telle que :*
- $|A|, |B| \leqslant 2n/3$
- *aucune arête de $G$ ne relie les parties $A$ et $B$*
- $|T| \leqslant O(\sqrt{n})$.

Pour un graphe dessiné sur une surface de rang $g$ le théorème reste valide avec $|T| \leqslant O(\sqrt{gn})$.

**11.12. — Lemme [6].** *Si l'ensemble des qubits (physiques) d'un code (stabilisateur ?) de q-dimension $k$ est partitionné en $A \sqcup T \sqcup B$ tels que les parties $A$ et $B$ soient corrigibles alors $k \leqslant |T|$.*

## Anyons [12]

Un code topologique peut aussi être défini comme l'espace minimisant l'hamiltonien :

$$H := \frac{1}{2}\Big( \sum_{v \in V} (1 - X_v) + \sum_{f \in F} (1 - Z_f) \Big)$$

où $X_v$ est l'opérateur en $X$ correspondant au cocycle élémentaire $v$ et $Z_f$ l'opérateur en $Z$ au cycle élémentaire $f$. On trouve le terme d'« états fondamentaux » pour les états quantiques appartenant au code, et d'« états excités » pour les états violant un ou plusieurs syndromes $X_v$ et $Z_f$. Pour le code torique de Kitaev, il y a 4 classes homologiques (éléments de la base logique) que certains notent $|\emptyset\rangle$, $|m\rangle$, $|l\rangle$ et $|d\rangle$ où le premier correspond à la classe homologique triviale, et les autres aux boucles horizontale, verticale et composée.

Une « charge électrique » en $v \in V$ correspond à un syndrome $X_v$ non-trivial. (Une charge ne vient jamais seule puisque le produit des $X_v$ est $I$.) Deux charges électriques peuvent être annulées en phase-flippant le long d'un chemin joignant les deux charges (ce procédé de correction d'erreur ne dépend pas du choix du chemin de même homologie). Une « charge magnétique » en $f \in F$ correspond à un syndrome $Z_f$ non-trivial. Deux charges magnétiques peuvent être annulées en bit-flippant le long d'un chemin joignant les deux charges dans le graphe dual.

On peut donc « déplacer » une charge sans changer la valeur logique de l'état. Mais si ce déplacement se fait le long d'une boucle fermée, autour d'une unique charge de l'autre type, il fait apparaitre un déphasage global de $-1$, puisque la boucle croise nécessairement un chemin joignant la charge encerclée à une autre de même type.

Plus généralement, pour des codes définis sur une surface orientée, on peut envisager plusieurs types de charges et décrire ce qu'il se passe lors de la fusion de deux charges ou lors de mouvements relatifs entre ces charges. Lorsque deux charges de même type $a$ sont interchangées par un mouvement de demi-révolution dans le sens direct, on obtient le même état, à une phase globale près souvent notée $\theta_a$. Lorsque deux charges de types $a$ et $b$ sont soumises à une mouvement de révolution complète dans le sens direct, on obtient le même état, à une phase globale près souvent notée $\mu_{a,b}$. On peut voir qu'on a les relations

$$\theta_{a\times b} = \theta_a\,\theta_b\,\mu_{a,b} \qquad \text{et} \qquad \mu_{a\times b,c} = \mu_{a,c}\,\mu_{b,c}$$

où $a \times b$ désigne la charge obtenue par fusion de $a$ et $b$.

## 12. Codes de Floquet

### Exemple simplifié de qubit dynamique

Soient $A$ et $B$ les codes *bit-flip* et *phase-flip*, de stabilisateurs respectifs

$$\mathcal{S}_A = \langle ZZI, IZZ\rangle \qquad \text{et} \qquad \mathcal{S}_B = \langle XXI, IXX\rangle.$$

Si on choisit les bases suivantes pour ces deux codes:

$$|\hat{\mathbf{0}}\rangle_A = |000\rangle \qquad |\hat{\mathbf{0}}\rangle_B = \frac{1}{\sqrt{2}}\big(|+++\rangle + |---\rangle\big) = \frac{1}{2}\sum_{\substack{a,b,c=0\\ a+b+c \text{ pair}}}^{1} |abc\rangle$$

et

$$|\hat{\mathbf{1}}\rangle_A = |111\rangle \qquad |\hat{\mathbf{1}}\rangle_B = \frac{1}{\sqrt{2}}\big(|+++\rangle - |---\rangle\big) = \frac{1}{2}\sum_{\substack{a,b,c=0\\ a+b+c \text{ impair}}}^{1} |abc\rangle$$

alors les opérateurs logiques

$$\hat{Z} = ZZZ \qquad \text{et} \qquad \hat{X} = XXX$$

leurs sont communs. En conséquence ($\hat{Z}$ commute avec $\mathcal{S}_A$ donc avec $\Pi_{++}$), l'opérateur de projection

$$\Pi_{++} = \left(\frac{III + ZZI}{2}\right)\left(\frac{III + IZZ}{2}\right)$$

sur le code A vérifie

$$\Pi_{++}\,|\hat{\mathbf{0}}\rangle_B = \frac{1}{2}|\hat{\mathbf{0}}\rangle_A \qquad \text{et} \qquad \Pi_{++}\,|\hat{\mathbf{1}}\rangle_B = \frac{1}{2}|\hat{\mathbf{1}}\rangle_A.$$

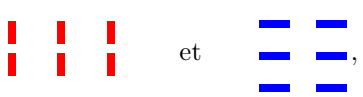
Donc, si on part d'un état $|\hat{q}\rangle_B = \alpha|\hat{\mathbf{0}}\rangle_B + \beta|\hat{\mathbf{1}}\rangle_B$ du code $B$, qu'on lui applique $2\Pi_{++}$ (on mesure selon $ZZI$ et $IZZ$ et on post-sélectionne sur les issues $+1$) alors on obtient l'état $\alpha|\hat{\mathbf{0}}\rangle_A + \beta|\hat{\mathbf{1}}\rangle_A$. L'information quantique est préservée. Au lieu de post-sélectionner, on peut corriger, c'est-à-dire appliquer

$$\Pi_{++} + IXX\cdot\Pi_{-+} + XXI\cdot\Pi_{+-} + XIX\cdot\Pi_{--}.$$

### Le code FBS

C'est le code de Floquet-Bacon-Shor introduit par [1] puis dont l'implémentation est rapportée dans [38]. Il protège un qubit logique statique (celui du code de Bacon), mais aussi un qubit dynamique porté par les qubits de jauge.

Je reprends le cas particulier où la taille du tableau est $d = 3$. Au lieu de mesurer alternativement selon les deux jauges $\mathcal{S}_X$ et $\mathcal{S}_Z$



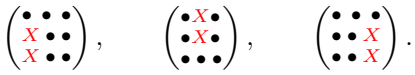
et



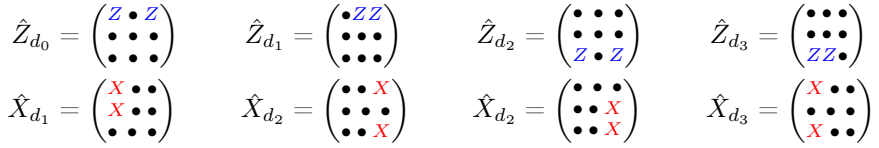
,

(où ▮ et ▬ représentent les « fragments » de poids 2, respectivement en $X$ et en $Z$), on utilise quatre jauges partielles

de façon séquentielle. Le stabilisateur instantané (ISG) est, après la mesure par la jauge de gauche (par exemple), engendré par $\mathcal{S}$ et par



Les opérateurs logiques pour le qubit dynamique sont successivement représentés par :



Le qubit statique reste protégé par une distance 3 (en général $d$). Le qubit dynamique est protégé par une distance 2 donc seulement en détection (en général par une distance $\simeq d/2$).

## Code hexagonal de Floquet

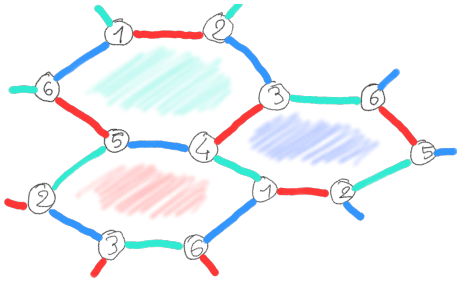
Le groupe de jauge est égal au centralisateur de $\mathcal{S}$ en entier, donc il n'y a pas de qubits statiquement protégés. Mais le stabilisateur varie de façon périodique et il y a donc des qubits protégés dynamiquement. L'exemple le plus connu est la version hexagonale du code torique [19][37].

Le tore est pavé avec $n$ cellules hexagonales. On peut colorer les cellules avec 3 couleurs $x$, $y$, $z$ de telle sorte que les cellules adjacentes soient de couleurs distinctes. On peut aussi colorer les arêtes (il y en a $3n$) de telle sorte qu'une cellule de couleur donnée soit entourée de 3 arêtes de chacune des deux autres couleurs, et que les arêtes adjacentes soient de couleurs différentes.

Les sommets (points de rencontre de trois cellules) correspondent aux qubits ; il y en a $2n$. On attribue aux arêtes les opérateurs de jauge $XX$, $YY$, ou $ZZ$ selon leur couleur : il y a $3n$ opérateurs de jauge (non indépendants ; leur produit est trivial) qui engendrent le groupe de jauge $\mathcal{G}$. Les six arêtes bordant chaque cellule sont donc associées à un opérateur de poids 6, qui est dans le centre de $\mathcal{G}$. Cet opérateur cellule a la couleur initialement attribuée à la cellule (en vertu de $XY \sim Z$, etc). Il y a $n-1$ opérateurs cellule indépendants (il y en a $n$ mais le produit d'entre eux est trivial). Les deux chemins d'homotopie non-triviale sur le tore définissent deux opérateurs qui sont dans le centre de $\mathcal{G}$ (en particulier ils commutent entre eux). Le stabilisateur « statique » $\mathcal{S}$ est donc de rang $n+1$, ce qui définit un code statique à $n-1$ qubits (logiques + jauge). En fait, $(3n-1)-(n+1) = 2(n-1)$ opérateurs de jauge indépendants de $\mathcal{S}$ s'organisent en paires d'opérateurs logiques pour $n-1$ qubits de jauge. Il ne reste donc aucun qubit logique (statique).

Les opérateurs de jauge sont évalués par familles successives. Le groupe stabilisateur dynamique (ISG) varie à chaque étape. Il est engendré par la dernière famille d'arêtes mesurées et par les opérateurs cellule. Il y a $2n-2$ générateurs indépendants (le produit de tous les opérateurs cellule est trivial, ainsi que le produit des opérateurs arêtes de la dernière couleur avec les opérateurs cellule de cette même couleur). Le code stabilisé par l'ISG définit donc 2 qubits logiques.

**Exemple avec $n = 3$**



Pour ce graphe torique à 6 sommets, 9 arêtes et 3 facettes, les opérateurs de jauge sont :

$$\begin{aligned} -XIIIIX, \quad -IXXIII, \quad -IIIXXI, \qquad &\text{(arêtes bleues)} \\ -YIIYII, \quad -IYIIYI, \quad -IIYIIY, \qquad &\text{(arêtes vertes)} \\ -ZZIIII, \quad -IIZZII, \quad -IIIIZZ. \qquad &\text{(arêtes rouges)} \end{aligned}$$

Les opérateurs facettes sont :

$$F_X = -XXXXXX, \quad F_Y = -YYYYYY, \quad F_Z = -ZZZZZZ$$

(les signes sont choisis pour que $F_X F_Y F_Z = +I^{\otimes 6}$) et on peut représenter les lacets non-triviaux par les opérateurs

$$L_Z = -IIXYYX, \quad L_Y = -ZIXXIZ, \quad L_X = -ZIIZYY$$

qui sont obtenus en suivant respectivement les chemins $(4,3,6,5,4)$, $(4,1,6,3,4)$ et $(4,5,6,1,4)$.

Le stabilisateur statique $\mathcal{S}$ est engendré par les opérateurs facettes (2 indépendants) et les opérateurs lacets (2 indépendants). Il définit un espace stabilisé de 2 qubits mal protégés, dont les opérateurs logiques peuvent être représentés par ($ZZIIII$, $IXXIII$) et ($IIIIZZ$, $IIIXXI$).

L'ISG est engendré par les opérateurs facettes et par les opérateurs de jauge de la dernière couleur mesurée (deux indépendants des facettes). Il est aussi de rang 4 ; il définit deux qubits logiques. Les opérateurs logiques associés à ces deux qubits sont représentés par deux opérateurs lacets (opérateurs logiques intérieurs), disons $\hat{Z}_1 = L_Z$ et $\hat{Z}_2 = L_Y$, et par deux opérateurs logiques extérieurs, qui dépendent de l'étape. Des choix possibles sont (aux signes près) :

$$\begin{aligned} \hat{X}_1 = IIXXII \quad &\text{et} \quad \hat{X}_2 = IIIZZI \qquad \text{(étape rouge)}, \\ \hat{X}_1 = IZIIZI \quad &\text{et} \quad \hat{X}_2 = IIIYYI \qquad \text{(étape bleue)}, \\ \hat{X}_1 = YIIIIY \quad &\text{et} \quad \hat{X}_2 = IIXIIX \qquad \text{(étape verte)}. \end{aligned}$$

Ces choix respectent la contrainte que $\hat{X}_1$ et $\hat{X}_2$ soient compatibles avec l'étape courante et l'étape suivante (dans l'ordre rouge → bleue → verte → rouge). On voit que le code obtenu est de distance 2 (le poids minimal des opérateurs logiques), ce qui n'est malheureusement pas mieux qu'en version statique.

D'autre part, puisque j'ai choisi $\hat{Z}_1$ et $\hat{Z}_2$ dans $\mathcal{S}$, le code statique (stabilisé par $\mathcal{S}$) est l'ensemble des états représentant la valeur logique $|00\rangle$, quelle que soit l'étape. Les états fixés par respectivement la jauge rouge, bleue et verte sont (merci `Magma`) :

$$|00\rangle_Z = \frac{1}{2\sqrt{2}}\big(|010101\rangle + |010110\rangle + |011001\rangle - |011010\rangle + |100101\rangle - |100110\rangle - |101001\rangle - |101010\rangle\big)$$

$$|00\rangle_X = \frac{1}{\sqrt{32}}\begin{pmatrix} |000001\rangle - |000010\rangle + |000100\rangle - |000111\rangle - |001000\rangle - |001011\rangle + |001101\rangle + |001110\rangle \\ +|010000\rangle + |010011\rangle - |010101\rangle - |010110\rangle - |011001\rangle + |011010\rangle - |011100\rangle + |011111\rangle \\ -|100000\rangle + |100011\rangle - |100101\rangle + |100110\rangle + |101001\rangle + |101010\rangle - |101100\rangle - |101111\rangle \\ -|110001\rangle - |110010\rangle + |110100\rangle + |110111\rangle + |111000\rangle - |111011\rangle + |111101\rangle - |111110\rangle \end{pmatrix}$$

$$|00\rangle_Y = \frac{1}{\sqrt{32}}\begin{pmatrix} |000001\rangle - |000010\rangle + |000100\rangle - |000111\rangle - |001000\rangle - |001011\rangle + |001101\rangle + |001110\rangle \\ +|010000\rangle + |010011\rangle + |010101\rangle + |010110\rangle + |011001\rangle - |011010\rangle - |011100\rangle + |011111\rangle \\ -|100000\rangle + |100011\rangle + |100101\rangle - |100110\rangle - |101001\rangle - |101010\rangle - |101100\rangle - |101111\rangle \\ -|110001\rangle - |110010\rangle + |110100\rangle + |110111\rangle + |111000\rangle - |111011\rangle + |111101\rangle - |111110\rangle \end{pmatrix}$$

et on a donc $|00\rangle_Y - |00\rangle_X = 2|00\rangle_Z$.

Le code fixé par l'ISG rouge est engendré par

$$\frac{1}{\sqrt{2}}\big(|010101\rangle - |101010\rangle\big),\ \frac{1}{\sqrt{2}}\big(|010110\rangle - |101001\rangle\big),\ \frac{1}{\sqrt{2}}\big(|011001\rangle - |100110\rangle\big),\ \frac{1}{\sqrt{2}}\big(|011010\rangle - |100101\rangle\big).$$

Si on part (par exemple) de l'état $|ab\rangle_Z$ et qu'on le mesure avec les opérateurs de jauge en $X$. On peut corriger en fonction du syndrome obtenu avec des opérateurs de jauge en $Z$ (ou en $Y$) pour ramener l'état dans le code stabilisé par le nouvel ISG. L'état ainsi obtenu est alors $|ab\rangle_X$ (car les opérateurs lacets $\hat{Z}_1$ et $\hat{Z}_2$ n'ont pas été impliqués) : l'information quantique des deux qubits logiques est préservée.

## 13. Bibliographie


[1] M.S. Alam, E. Rieffel : *Dynamical logical qubits in the Bacon-Shor code.* arXiv:2403.03291v2 [quant-ph] (2024).

[2] P. Aliferis, A.W. Cross : *Subsystem fault tolerance with the Bacon-Shor code.* Physical Review Letters 98, 220502 (2007).

[3] H. Bombín : *An introduction to topological quantum codes.* arXiv:1311.0277 [quant-ph] (2013).

[4] H. Bombín, M.A. Martín-Delgado : *Topological quantum distillation.* Physical Review Letter 97, 180501 (2006).

[5] H. Bombín, M.A. Martín-Delgado : *Homological error correction: classical and quantum codes.* Journal of Mathematical Physics 48, 052105 (2007).

[6] S. Bravyi, D. Poulin, B. Terhal : *Tradeoffs for reliable quantum information storage in 2D systems.* Physical Review Letters 104, 050503 (2010).

[7] S. Bravyi, B. Terhal : *A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes.* New Journal of Physics 11, 043029 (2009).

[8] N.P. Breuckmann : *Homological quantum codes beyond the toric code.* PhD dissertation, 2017.

[9] R.K. Brylinski, G. Chen : *Mathematics of Quantum Computation.* Chapman & Hall/CRC (2002).

[10] R. Cleve, D. Gottesman, H.-K. Lo : *How to share a quantum secret.* Physical Review Letters 83, 648 (1999).

[11] A. Cross, G. Smith, J.A. Smolin, B. Zeng : *Codeword stabilizer quantum codes.* IEEE Transactions on Information Theory 55, 433–438 (2009).

[12] S.X. Cui : *Topological Quantum Computation.* Stanford University course (2018).

[13] S.J. Devitt, W.J. Munro, K. Nemoto : *Quantum Error Corrrection for Beginners.* arXiv:0905.2794 [quant-ph] (2009–2013).

[14] V. Gheorghiu : *Standard form of qudit stabilizer group.* Physics Letters A 378, 505–509 (2014).

[15] D. Gottesman : *Stabilizer codes and quantum error correction.* arXiv:quant-ph/9705052 (thesis, 1997).

[16] D. Gottesman : *Theory of fault tolerant computation.* Physical Review A 57, 127 (1998).

[17] D. Grier, L. Schaeffer : *The classification of Clifford gates over qubits.* Quantum 6, 734 (2022).

[18] J. Haah : *A degeneracy bound for homogeneous topological order.* SciPost Phys. 10, 011 (2021).

[19] M.B. Hastings, J. Haah : *Dynamically generated logical qubits.* Quantum 5, 564 (2021).

[20] M. Hein, J. Eisert, H.J. Briegel : *Multiparty entanglement in graph states.* Physical Review A 69, 062311 (2004).

[21] M.S. Kesselring, F. Pastawski, J. Eisert, B.J. Brown : *The boundaries and twist defects of the color code and their applications to topological quantum computation.* Quantum 2, 101 (2018).

[22] E. Knill, R. Laflamme, R. Martinez, C. Negrevergne : *Benchmarking quanum computers: the five-qubit error correcting code.* Physical Review Letters 86, 5811.

[23] A.A. Kovalev, I. Dummer, L.P. Pryadko : *Design of additive quantum codes via the code-word-stabilized framework.* Physical Review A 84, 062319 (2011).

[24] A.A. Kovalev, L.P. Pryadko : *Quantum Kronecker sum-product low-density parity-check codes with finite rate.* Physical Review A 88, 012311 (2013).

[25] A.A. Kovalev, L.P. Pryadko : *Improved quantum hypergraph-product LDPC codes.* IEEE-IT (2012).

[26] R. Laflamme, C. Miquel, J.P. Paz, W.H. Zurek : *Perfect quantum error correcting code.* Physical Review Letters 77, 198 (1996).

[27] H.-K. Lin, L.P. Pryadko : *Quantum two-block group algebra codes.* arXiv:2306.16400 (2023).

[28] S.Y. Looi, L. Yu, V. Gheorghiu, R.B. Griffiths : *Quantum-error-correcting codes using qudit graph states.* Physical Review A 78, 042303 (2008).

[29] R. Majumdar, S. Basu, S. Ghosh, S. Sur-Kolay : *Quantum error-correcting code for ternary logic.* Physical Review A 97, 052302 (2018).

[30] M.A. Nielsen, I.L. Chuang : *Quantum Computation and Quantum Information.* Cambridge University Press (2000/2011).

[31] P. Panteleev, G. Kalachev : *Degenerate quantum LDPC codes with good finite length performance.* Quantum 5, 585 (2021).

[32] P. Panteleev, G. Kalachev : *Quantum LDPC Codes With Almost Linear Minimum Distance.* IEEE Transactions on Information Theory 68, 213 (2022).

[33] J. Preskill : *Lecture Notes for Physics 229: Quantum Information and Computation.* `http://www.theory.caltech.edu/people/preskill/ph229`.

[34] B. Shaw, M.M. Wilde, O. Oreshkov, I. Kremsky, D.A. Lidar : *Encoding one logical qubit into six physical qubits.* Physical Review A 78, 012337 (2008).

[35] P.W. Shor : *Scheme for reducing decoherence in quantum computer memory.* Physical Review A (Rapid Communications) 52, R2493 (1995).

[36] A. Steane : *Multiple-particle interference and quantum error correction.* Proc. R. Soc. Lond. A, 452, 2551–2577 (1996).

[37] M. Suchara, S. Bravyi, B. Terhal : *Constructions and noise threshold of topological subsystem codes.* Journal of Physics A 44, 155301 (2011).

[38] X. Sun, L. Li, Z. Wu and 29 more people : *Universal logical operations with a dynamical qubit in Floquet code.* arXiv2503.03867 [quant-ph] (2025).

[39] B. Terhal : *Quantum error correction for quantum memories.* Review of Modern Physics 87, 307 (2015).

[40] J.P. Tillich, G. Zémor : *Quantum LDPC codes with positive rate and minimum distance proportional to $n^{1/2}$.* In ISIT 2009, 799–803, IEEE International Symposium on Information Theory (2009).

[41] T.A. Walker, F.A.C. Polack, S.L. Braunstein : *Error correcting Bell inequalities.* Physics Review Letters 101, 080501 (2008).

[42] R. Wang, L.P. Pryadko : *Distance bounds for generalized bicycle codes.* Symmetry 14, 248 (2022).

[43] T.H. Yoder, R. Takagi, I.L. Chuang : *Universal fault-tolerant gates on concatenated stabilizer codes.* Physical Review X 6, 031039 (2016).