ENSEIRB-MATMECA- Section Informatique, 2ième année
Option second semestre, 2015/2016

Information Quantique

DM- à rendre avant le 25 Avril 2016, à midi

Partie I

Un code linéaire classique.

L'encodage $\varphi : F_2^4 \to F_2^7$ est défini par : pour tout vecteur ligne $w \in F_2^4$

$$\varphi(w) = w \cdot G.$$

1- Soit $y \in F_2^7$. Il existe un vecteur $w \in F_2^4$ tel que

$$y = w \cdot G$$

ssi $\exists w_1, w_2.w_3, w_4 \in F_2$ tels que

$$y_1 = w_1 \wedge y_2 = w_2 \wedge y_3 = w_3 \wedge y_4 = w_4 \text{ et}$$

$$y_5 = w_2 + w_3 + w_4 \wedge y_6 = w_1 + w_3 + w_4 \wedge y_7 = w_1 + w_2 + w_4$$

ce qui equivaut à

$$y_2 + y_3 + y_4 + y_5 = 0; y_1 + y_3 + y_4 + y_6 = 0; y_1 + y_2 + y_4 + y_7 = 0; \quad (1)$$

2- Soit

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

D'après (1), pour tout $y \in F_2^7$,

$$y \in C \Leftrightarrow H \cdot \ {}^t y = 0.$$

3- Soit $S : F_2^7 \to F_2^3$ l'application

$$S(y) := H \cdot \ {}^t y.$$

D' après la question 2, $\mathrm{Ker}(S) = C$.
Comme $S(e_5), S(e_6), S(e_7)$ est la base canonique de F_2^3, on a aussi que $Im(S) = F_2^3$.

Par le théorème de factorisation des applications linéaires on en conclut que : $\bar{S} : F_2^7/C \to F_2^3$ telle que

$$\bar{S}(y + C) = S(y)$$

est un isomorphisme. Or $\bar{S}$ est exactement l'application syndrome.
4- 4.1 Calculons la table des syndromes des vecteurs de poids ≤ 1 (elle découle immédiatement de la matrice H) :

vect$(s)\backslash e$:	$\overrightarrow{0}$	e_1	e_2	e_3	e_4	e_5	e_6	e_7
s_1	0	0	1	1	1	1	0	0
s_2	0	1	0	1	1	0	1	0
s_3	0	1	1	0	1	0	0	1

4.2 On vérifie que les syndromes des 8 vecteurs de poids ≤ 1 sont tous distincts.
5- Considérons les applications

$$0 \to F_2^4 \stackrel{\varphi}{\to} F_2^7 \stackrel{S}{\to} F_2^3 \to 0$$

N.B. chaque image d'une flèche est le noyau de la flèche juste à sa droite.
Remarquons que φ est injective et S est surjective.
Définissons : $\varphi^{-1} : C \to F_2^4$ comme la réciproque de φ (dont l'image est restreinte à C)

$$\mathrm{Dom}(\varphi^{-1}) = \mathrm{C}, \forall \mathrm{c} \in \mathrm{C}, \varphi(\varphi^{-1}(\mathrm{c})) = \mathrm{c}, \forall \mathrm{u} \in \mathrm{F}_2^4, \varphi^{-1}(\varphi(\mathrm{u})) = \mathrm{u}$$

et $\bar{S} : F_2^3 \to F_2^7$ comme l'application "inverse" de S restreinte aux vecteurs de poids ≤ 1 :

$$\forall u \in F_2^3, \ \ \mathrm{wt}(\bar{\mathrm{S}}(\mathrm{u})) \leq 1 \text{ et } \mathrm{S}(\bar{\mathrm{S}}(\mathrm{u})) = \mathrm{u}. \tag{2}$$

On pose alors

$$\forall u \in F_2^7, \ \ \bar{\varphi}(u) := \varphi^{-1}(u + \bar{S}(S(u))). \tag{3}$$

N.B. $\bar{\varphi}(u)$ est indéfini lorsque $u + \bar{S}(S(u)) \notin C$.
Soit $w \in F_2^4$ $e \in F_2^7$ de poids ≤ 1.

$$\begin{aligned}
\bar{\varphi}(\varphi(w) + e) = \ & \varphi^{-1}(\varphi(w) + e + \bar{S}(S(\varphi(w) + e))) & \\
= \ & \varphi^{-1}(\varphi(w) + e + \bar{S}(S(e))) & (\text{ car } \bar{S}(S(\varphi(w))) = 0 \\
= \ & \varphi^{-1}(\varphi(w) & (\text{ car } e = \bar{S}(S(e))) \\
= \ & w &
\end{aligned}$$

Partie II

Groupes de Pauli.

Notons $\mathcal{M}_4 := \{I, X, Y, Z\}$ et $C_4 := \{+1, -1, i, -i\}$.
Avec ces notations :

$$\mathbb{P} := C_4 \cdot \mathcal{M}_4.$$

2- On vérifie que $X^2 = Y^2 = Z^2 = I$.
Pour chaque $M \in \{X, Y, Z\}$, les valeurs propres de M sont des racines de $X^2 - 1$, donc $Spec(M) \subseteq \{+1, -1\}$.
Par ailleurs $M \notin \{I, -I\}$ donc $Spec(M) = \{+1, -1\}$.
1- On calcule les produits :

$$XY = iZ, \;\; YZ = iX, \;\; ZX = iY.$$

On en déduit, par exemple, le produit en ordre inverse : $YX = (-iZX) \cdot X = -iZ$
et, finalement, par trois manipulations analogues

$$YX = -iZ, \;\; ZY = -iX, \;\; XZ = -iY.$$

On en déduit que pour tous $\alpha, \beta \in C_4$,

$$(\alpha X)(\beta Y) = (i\alpha\beta)Z, \;\; (\alpha Y)(\beta Z) = (i\alpha\beta)Z, \;\; (\alpha Z)(\beta X) = (i\alpha\beta)Y$$

$$(\alpha Y)(\beta X) = (-i\alpha\beta)Z, \;\; (\alpha Z)(\beta Y) = (-i\alpha\beta)Z, \;\; (\alpha X)(\beta Z) = (-i\alpha\beta)Y.$$

et C_4 est clos par produit. Donc $\mathbb{P}$ est clos par produit.
On vérifie aussi que : pour tous $\alpha \in C_4, M \in \mathcal{M}_4$

$$(\alpha M)^{-1} = (\alpha)^{-1} M^{-1} \in \mathbb{P}.$$

Donc $\mathbb{P}$ est clos par inverse.
Finalement, $\mathbb{P}$ est une partie non-vide de $U(2)$ close par produit et inverse : c' est un sous-groupe de $U(2)$.
3- D'après la question 1 :
- si $P, Q \in \{X, Y, Z\}$ et $P \neq Q$, alors $PQ = -QP$
- si $P, Q \in \{X, Y, Z, I\}$ et ($P = Q$ ou $P = I$ ou $Q = I$), alors $PQ = QP = I$.
Comme les coefficients $\alpha, \beta \in C_4$ commutent avec les matrices de $\mathcal{M}_4$ on en conclut que, pour tous $P, Q \in \mathbb{P}$, il existe $\varepsilon \in \{+1, -1\}$ tel que $PQ = \varepsilon QP$ i.e.

$$P^{-1}QP = \varepsilon Q.$$

4- Soient $P, Q \in \mathbb{P}$, et $|u\rangle$ vecteur propre de Q, pour une valeur propre $\lambda \in \mathbb{C}$. Alors, il existe $\varepsilon \in \{+1, -1\}$ tel que :

$$\begin{aligned} Q(P\,|u\rangle) &= (QP)\,|u\rangle \\ &= \varepsilon(PQ)\,|u\rangle \quad (\text{ par la question 3}) \\ &= \varepsilon P(\lambda\,|u\rangle) \quad (|u\rangle \text{ est v. propre de } Q) \\ &= (\varepsilon\lambda)P\,|u\rangle \end{aligned}$$

Comme P est inversible et $|u\rangle \neq 0$, $P\,|u\rangle$ est non-nul : c'est bien un vecteur propre de Q (pour la valeur propre $\varepsilon\lambda$).
5- Les coordonnés (en ligne) des matrices I, X, Y, Z dans la base canonique de $\mathbb{M}_{2,2}(\mathbb{C})$ forment la matrice $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & -i & i & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}$ dont le déterminant vaut :

$$\begin{vmatrix} 1 & 1 & 0 \\ -i & i & 0 \\ 0 & 0 & -1 \end{vmatrix} - \begin{vmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ -i & i & 0 \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ -i & i \end{vmatrix} \cdot (-1) - \begin{vmatrix} 1 & 1 \\ -i & i \end{vmatrix} = -4i.$$

Ces quatres matrices sont donc linéairement indépendantes, et comme la dimension de $\mathbb{M}_{2,2}(\mathbb{C})$ vaut 4, elles forment une *base* de $\mathbb{M}_{2,2}(\mathbb{C})$.
6- Soient $P, Q \in \mathbb{P}_n$:

$$P = P_1 \otimes \cdots \otimes P_k \otimes \cdots \otimes P_n, \;\; Q = Q_1 \otimes \cdots \otimes Q_k \otimes \cdots \otimes Q_n. \qquad (4)$$

Alors

$$P \cdot Q = P_1Q_1 \otimes \cdots \otimes P_kQ_k \otimes \cdots \otimes P_nQ_n \text{ et}$$

$$P^{-1} = P_1^{-1} \otimes \cdots \otimes P_k^{-1} \otimes \cdots \otimes P_n^{-1}.$$

Comme pour tout $k \in [1, n], P_kQ_k \in \mathbb{P}$, $P \cdot Q$ est bien un élément de $\mathbb{P}_n$. De même, comme pour tout $k \in [1, n], P_k^{-1} \in \mathbb{P}$, P^{-1} est bien un élément de $\mathbb{P}_n$. Finalement, $\mathbb{P}_n$ est un sous-groupe du groupe unitaire de dimension 2^n.
7- Soient P, Q de la forme (4). Pour tout $k \in [1, n]$, il existe $\varepsilon_k \in \{+1, -1\}$ tel que $P_k^{-1}Q_kP_k = \varepsilon_kQ_k$ (par la question 3). Donc

$$P^{-1}QP = (\prod_{k=1}^{n} \varepsilon_k)Q.$$

Comme à la question 4, on en conclut que, si $|u\rangle$ vecteur propre de Q, alors $P|u\rangle$ est vecteur propre de Q.
8- L'ensemble $\mathcal{M}_4$ est une base de $\mathbb{M}_{2,2}(\mathbb{C})$ (vu à la question 5).
Donc $\mathcal{M}_4 \otimes \cdots \otimes \mathcal{M}_4$ (produit tensoriel itéré n fois) est une base de $\mathbb{M}_{2,2}(\mathbb{C}) \otimes \cdots \otimes \mathbb{M}_{2,2}(\mathbb{C})$, qui est un sous-espace de dimension $4^n = 2^n \cdot 2^n$ de l' espace $\mathbb{M}_{2^n,2^n}(\mathbb{C})$ qui est aussi de dimension $2^n \cdot 2^n$. Donc

$$\mathcal{M}_4 \otimes \cdots \otimes \mathcal{M}_4 \text{ est une base de } \mathbb{M}_{2^n,2^n}(\mathbb{C}) \tag{5}$$

Soit B un élément de $\mathcal{M}_4 \otimes \cdots \otimes \mathcal{M}_4$:

$$B = M_1 \otimes \cdots \otimes M_k \otimes \cdots \otimes M_n$$

avec, pour tout $k \in [1, n]$, $M_k \in \mathcal{M}_4$.
Chaque matrice $B_k := I \otimes \cdots \otimes M_k \otimes \cdots \otimes I$ est un élément de $\mathbb{P}_n$ et $B = B_1 \cdots B_k \cdots B_n$. Donc $B \in \mathbb{P}_n$. Donc

$$\mathrm{Vect}_{\mathbb{C}}(\mathcal{M}_4 \otimes \cdots \otimes \mathcal{M}_4) \subseteq \mathrm{Vect}_{\mathbb{C}}(\mathbb{P}_n),$$

et comme, par (5), le membre gauche de cette inclusion est l'espace $\mathbb{M}_{2^n,2^n}(\mathbb{C})$, nous en concluons que :

$$\mathbb{M}_{2^n,2^n}(\mathbb{C}) = \mathrm{Vect}_{\mathbb{C}}(\mathbb{P}_n).$$

Partie III

Un premier code quantique.

Dans cette partie, on définit un code quantique permettant de corriger les erreurs de type "flip" .
On encode les qbit $|0\rangle$ (resp. $|1\rangle$) par

$$|\bar{0}\rangle := |000\rangle\,, \quad |\bar{1}\rangle := |111\rangle\,.$$

Un état général $\alpha|0\rangle + \beta|1\rangle$ (où $\alpha, \beta \in \mathbb{C}$) est encodé par

$$|\psi\rangle = \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle \tag{6}$$

On suppose que cet état a été "altéré" par une erreur (au plus) de type "flip" i.e. a été transformé en

$$|\psi'\rangle = P|\psi\rangle \text{ avec } P \in \{I, X_1, X_2, X_3\}.$$

1- 1.1 On vérifie aisément que $|\bar{0}\rangle, |\bar{1}\rangle$ sont des vecteurs unitaires, orthogonaux.
Le vecteur $|0\rangle$ est invariant par Z, donc

$$S_1|000\rangle = S_2|000\rangle = |000\rangle\,.$$

Pour le vecteur $|1\rangle$ on a

$S_1 |111\rangle = (-|1\rangle)\otimes(-|1\rangle)\otimes|1\rangle = |111\rangle$ et $S_2 |111\rangle = (|1\rangle)\otimes(-|1\rangle)\otimes(-|1\rangle) = |111\rangle$.

1.2 S_1, S_2 sont linéaires, donc l'ensemble de leurs vecteurs invariants est un sous-espace vectoriel. Comme $|\psi\rangle$ appartient au s.e.v. engendré par $|000\rangle, |111\rangle$, il est invariant par S_1 et par S_2.
1.3 $|\psi\rangle$ est vecteur propre de S_1 (pour $\lambda = 1$) et aussi de S_2 (pour $\lambda = 1$). Comme $X_1, X_2, X_3 \in \mathbb{P}_3$, par la question II.7, on conclut que $X_1 |\psi\rangle, X_2 |\psi\rangle, X_3 |\psi\rangle$ sont des vecteurs propres de S_1 et aussi de S_2.

On appelle "syndrome" de l'état erroné $|\psi'\rangle$ le couple $(\lambda_1, \lambda_2) \in \{+1, -1\}^2$ tel que

$$S_1 |\psi'\rangle = \lambda_1 |\psi'\rangle, \quad S_2 |\psi'\rangle = \lambda_2 |\psi'\rangle,$$

autrement dit, ce sont les valeurs propres pour lesquelles $|\psi'\rangle$ est vecteur propre.

2- Remplissons le tableau des syndromes :

$\lambda \backslash \|\psi'\rangle$	$I\|\psi\rangle$	$X_1\|\psi\rangle$	$X_2\|\psi\rangle$	$X_3\|\psi\rangle$
λ_1	$+1$	-1	-1	$+1$
λ_2	$+1$	$+1$	-1	-1

On utilise le fait que, pour tout $k, \ell \in [1, 3]$ tels que $k \neq \ell$

$$Z_k X_k = -X_k Z_k, \quad Z_\ell X_k = X_k Z_\ell.$$

Par exemple :

$S_1(X_1 |\psi\rangle) = Z_1 Z_2 X_1 |\psi\rangle = Z_1 X_1 Z_2 |\psi\rangle = -X_1 Z_1 Z_2 |\psi\rangle = -X_1(S_1 |\psi\rangle) = (-1)\cdot(X_1 |\psi\rangle)$.

On considère le circuit quantique suivant sur 5 qbits (voir la figure 1).
3- Soit $|u\rangle$ un état de $\mathcal{B}^{\otimes 3}$ qui est vecteur propre de S_j pour la valeur propre $\lambda_j = (-1)^{s_j}$ (pour chaque $j \in \{1, 2\}$). Calculons l'effet de la "partie haute" du circuit (H sur 4ieme qbit , $c - S_1$, H sur 4ieme qbit) sur $|u\rangle |0\rangle$:

$$\begin{aligned}
|u\rangle |0\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}} |u\rangle (|0\rangle + |1\rangle) \\
&\xrightarrow{c-S_1} \frac{1}{2}[|u\rangle |0\rangle + S_1 |u\rangle |1\rangle] \\
&\xrightarrow{H} \frac{1}{2}[|u\rangle (|0\rangle + |1\rangle) + S_1 |u\rangle (|0\rangle - |1\rangle)] \\
&= \frac{1}{2}[(|u\rangle + S_1 |u\rangle) |0\rangle + (|u\rangle - S_1 |u\rangle) |1\rangle
\end{aligned}$$

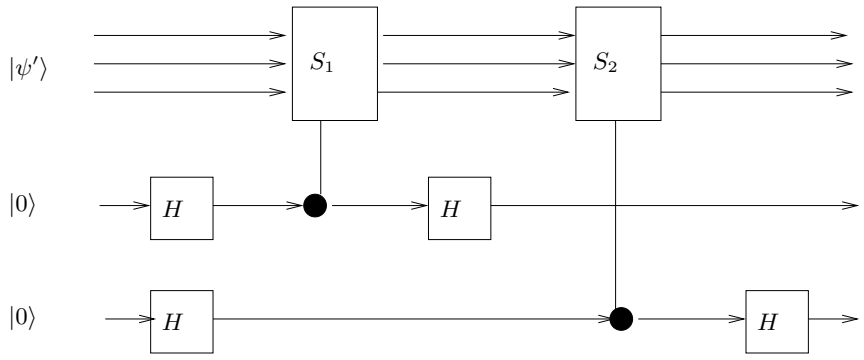

FIGURE 1 – Circuit détectant un flip

Donc :
- si $\lambda_1 = 1$, i.e. $s_1 = 0$, on obtient $|u\rangle\,|0\rangle$
- si $\lambda_1 = -1$, i.e. $s_1 = 1$, on obtient $|u\rangle\,|1\rangle$

L'effet de la "partie basse" du circuit (H sur 5ieme qbit , $c - S_2$, H sur 5ieme qbit) sur un vecteur $|u\rangle\,|s\rangle\,|0\rangle$ est, de facon analogue :
- si $\lambda_2 = 1$, i.e. $s_2 = 0$, on obtient $|u\rangle\,|s\rangle\,|0\rangle$
- si $\lambda_2 = -1$, i.e. $s_2 = 1$, on obtient $|u\rangle\,|s\rangle\,|1\rangle$.

On a vu à la question 2 que $|\psi\rangle'$ est vecteur propre de S_j avec comme valeurs propres les syndromes. L'enchainement de ces deux circuits produit donc successivement : $|\psi\rangle'\,|s_1\rangle\,|0\rangle$ puis

$$|\psi\rangle'\,|s_1\rangle\,|s_2\rangle\,.$$

4- Il suffit de construire un circuit sur 5 q-bits qui calcule :

$$|u\rangle\,|s_1\rangle\,|s_2\rangle \mapsto X(s_1,s_2)\,|u\rangle\,|0\rangle\,|0\rangle\,,$$

avec $X(0,0) = I, X(1,0) = X_1, X(1,1) = X_2, X(0,1) = X_3$.
N.B. $X(s_1,s_2)$ est l'erreur qui a produit le syndrome $((-1)^{s_1},(-1)^{s_2})$), et aussi l'opérateur qui corrige cette erreur. Une fois l'erreur *détectée* par le circuit de la figure (1), le circuit quantique de la figure (2) la *corrige* :

Partie IV

Code de Shor.

Dans cette partie, on définit un code quantique permettant de corriger *toute* erreur commise sur un seul qbit (sur un total de 9 qbits). On considère les

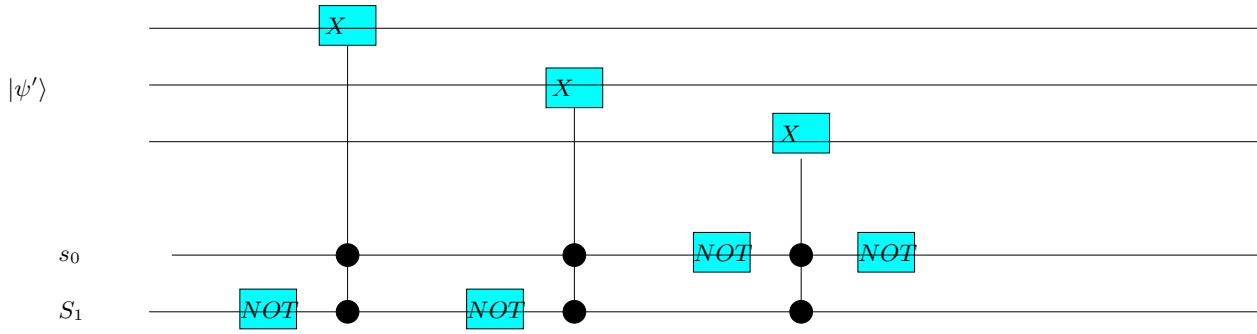

FIGURE 2 – Circuit corrigeant un flip

8 éléments du groupe $\mathbb{P}_3$:

$S_1 := Z_1 \cdot Z_2$, $S_2 := Z_2 \cdot Z_3$. $S_3 := Z_4 \cdot Z_5, S_4 := Z_5 \cdot Z_6$. $S_5 := Z_7 \cdot Z_8$, $S_6 := Z_8 \cdot Z_9$.

$$S_7 := X^{\otimes 6} \otimes I^{\otimes 3}, \quad S_8 := I^{\otimes 3} \otimes X^{\otimes 6}.$$

On encode les qbit $|0\rangle$ (resp. $|1\rangle$) par

$$|\bar{0}\rangle := (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle \otimes (|000\rangle + |111\rangle)$$

$$|\bar{1}\rangle := (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle \otimes (|000\rangle - |111\rangle).$$

Soit

$$|\psi\rangle = \alpha\,|\bar{0}\rangle + \beta\,|\bar{1}\rangle \tag{7}$$

1- 1.1 On vérifie que

$$\langle 0^3 + 1^3 | 0^3 - 1^3 \rangle = \langle 0^3 | 0^3 \rangle - \langle 1^3 | 1^3 \rangle = 1 - 1 = 0$$

Comme $|\bar{0}\rangle = (|0^3\rangle + |1^3\rangle)^{\otimes 3}$ et $|\bar{1}\rangle = (|0^3\rangle - |1^3\rangle)^{\otimes 3}$, on en déduit que

$$\langle \bar{0} | \bar{1} \rangle = 0.$$

Par des calculs analogues on calcule :

$$\langle \bar{0} | \bar{0} \rangle = 8, \quad \langle \bar{1} | \bar{1} \rangle = 8.$$

Donc les vecteurs $|\bar{0}\rangle, |\bar{1}\rangle$ sont orthogonaux et de norme $2\sqrt{2}$ [1]. On pourra choisir dans la suite de cette partie IV, le nouveau couple de vecteurs unitaires et orthogonaux :

$$|\bar{0}\rangle := \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle \otimes (|000\rangle + |111\rangle)$$

1. donc *non-unitaires*, erreur dans l'énoncé, mea culpa

$$|\bar{1}\rangle := \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle \otimes (|000\rangle - |111\rangle).$$

Invariance par les transformations S_j ($j \in [1,8]$) :
Z_1Z_2 (resp. Z_2Z_3) fixe les vecteurs de la base canonique de la forme $|000\rangle \otimes |v\rangle$ ou $|111\rangle \otimes |v\rangle$, pour $v \in \mathbb{B}^6$ (car un nombre pair de qbits est multiplié par (-1)).
De même Z_4Z_5 (resp. Z_5Z_6)fixe les vecteurs de la base canonique de la forme $|u\rangle \otimes |000\rangle \otimes |v\rangle$ ou $|u\rangle \otimes |111\rangle \otimes |v\rangle$, pour $u, v \in \mathbb{B}^3$,
et Z_7Z_8 (resp. Z_8Z_9) fixe les vecteurs de la base canonique de la forme $|u\rangle \otimes |000\rangle$ ou $|u\rangle \otimes |111\rangle$, pour $u \in \mathbb{B}^6$. Or $|\bar{0}\rangle, |\bar{1}\rangle$ sont dans le sous-espace engendré par les vecteurs de ces formes. Donc $|\bar{0}\rangle, |\bar{1}\rangle$ sont invariants par $S_1, S_2, S_3, S_4, S_5, S_6$.
Comme $|000\rangle + |111\rangle$ est fixé par $X \otimes X \otimes X$, le vecteur $|\bar{0}\rangle$ est fixé par S_7 et S_8.
$X_1X_2X_3$ envoie $(|000\rangle - |111\rangle) \otimes |v\rangle$ sur $-(|000\rangle - |111\rangle) \otimes |v\rangle$ (pour tout $v \in \mathbb{B}^6$), $X_4X_5X_6$ envoie $|u\rangle \otimes (|000\rangle - |111\rangle) \otimes |v\rangle$ sur $|u\rangle \otimes (-|000\rangle + |111\rangle) \otimes |v\rangle$ (pour tout $u, v \in \mathbb{B}^3$). Donc leur produit $S_7 = X_1X_2X_3X_4X_5X_6$ fixe tout vecteur de la forme :

$$(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes |\psi\rangle,$$

en particulier S_7 fixe $|\bar{1}\rangle$.
De même S_8 envoie le second (resp. troisième) bloc de $|\bar{1}\rangle$ sur son opposé, et donc fixe le vecteur $|\bar{1}\rangle$.
1.2 Par linéarité des S_j, $|\psi\rangle$ est invariant par toutes les transformations S_j ($j \in [1,8]$).
1.3 Comme $|\psi\rangle$ est vecteur propre des S_j, d' après QII.7, pour toute transformation $P \in \mathbb{P}_9$, $P|\psi\rangle$ est aussi vecteur propre des S_j ($j \in [1,8]$). En particulier, pour tout $k \in [1,9]$, les vecteurs $|\psi\rangle, X_k|\psi\rangle, Z_k|\psi\rangle, Y_k|\psi\rangle$ sont des vecteurs propres de toutes les transformations S_j ($j \in [1,8]$).

Soit $|\psi'\rangle = P|\psi\rangle$ où P (l'"erreur") est l'une des transformations I, X_k, Y_k, Z_k ($k \in [1,9]$). On appelle "syndrome" de l'état erroné $|\psi'\rangle$, le 8-uple $(\lambda_1, \ldots, \lambda_8) \in \{+1, -1\}^8$ tel que

$$\forall j \in [1,8], \quad S_j|\psi'\rangle = \lambda_j|\psi'\rangle.$$

2- Soit Q l'une des transformations S_j (pour un entier $j \in [1,8]$) et soit $\lambda_j \in \{+1, -1\}$ tel que $QPQ^{-1} = \lambda_j P$.

Alors

$$\begin{aligned} Q(P\,|\psi\rangle) &= (QPQ^{-1})(Q\,|\psi\rangle) \\ &= (QPQ^{-1})\,|\psi\rangle \quad (\text{ par la question 1.2 }) \\ &= \lambda_j(P\,|\psi\rangle) \end{aligned}$$

Le syndrome $(\lambda_j)_{j\in[1,8]}$ ne dépend donc que des $S_jPS_j^{-1}$: il est entièrement déterminé par P.
3- Calculons la table des syndromes pour les erreurs I ou X_k $(k \in [1,9])$:

$\lambda\backslash P$:	I	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9
λ_1	1	−1	−1	1	1	1	1	1	1	1
λ_2	1	1	−1	−1	1	1	1	1	1	1
λ_3	1	1	1	1	−1	−1	1	1	1	1
λ_4	1	1	1	1	1	−1	−1	1	1	1
λ_5	1	1	1	1	1	1	1	−1	−1	1
λ_6	1	1	1	1	1	1	1	1	−1	−1
λ_7	1	1	1	1	1	1	1	1	1	1
λ_8	1	1	1	1	1	1	1	1	1	1

puis la table des syndromes pour les erreurs Z_k, $(k \in [1,9])$ (nous les nommerons $(\mu_j)_{j\in[1,8]}$) :

$\mu\backslash P$:	I	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_7	Z_8	Z_9
μ_1	1	1	1	1	1	1	1	1	1	1
μ_2	1	1	1	1	1	1	1	1	1	1
μ_3	1	1	1	1	1	1	1	1	1	1
μ_4	1	1	1	1	1	1	1	1	1	1
μ_5	1	1	1	1	1	1	1	1	1	1
μ_6	1	1	1	1	1	1	1	1	1	1
μ_7	1	−1	−1	−1	−1	−1	−1	1	1	1
μ_8	1	1	1	1	−1	−1	−1	−1	−1	−1

4- Comme $Z_kX_k = iY_k$ on a aussi, pour tout $Q \in \mathbb{P}_9$:

$$QY_kQ^{-1} = -i(QZ_kQ^{-1})(QX_kQ^{-1})$$

En prenant $Q = S_j$ on obtient :

$$QY_kQ^{-1} = -i(\lambda_j(Z_k)Z_k)(\lambda_j(X_k)X_k) = \lambda_j(Z_k)\lambda_j(X_k)Y_k.$$

Le syndrome $\lambda_j(Y_k)$ calculé par l'opérateur S_j sur l'erreur Y_k, est donc :

$$\lambda_j(Y_k) = \lambda_j(Z_k) \cdot \lambda_j(X_k).$$

5- Le calcul du syndrome λ_k ($k \in [1,8]$) se fait en suivant la même méthode qu'à la question III.3 ; Le calcul du syndrome μ_k ($k \in [1,8]$) se fait aussi en suivant la même méthode qu'à la question III.3 ; L'enchainement des deux circuits, produit donc, à partir de $|\Psi\rangle' \otimes \left|0^8\right\rangle$ un état

$$|\Psi\rangle' \otimes |s_1 s_2 s_3 s_4 s_5 s_6 s_7 s_8\rangle$$

avec

$$\lambda_k = (-1)^{s_k} \text{ pour } k \in [1,6], \quad \mu_k = (-1)^{s_k} \text{ pour } k \in [7,8]$$

Si $|\Psi\rangle' = X_k |\psi\rangle$, le syndrome correspondant est codé dans $s_1, \dots s_6$
Si $|\Psi\rangle' = Z_k |\psi\rangle$, le syndrome correspondant est codé dans s_7, s_8
Si $|\Psi\rangle' = Y_k |\psi\rangle = iZ_kX_k |\psi\rangle$, le syndrome correspondant est codé dans $s_1, \dots, s_8$. Voir le circuit de la figure 3.

6- Pour corriger toute erreur de type X_k , il suffit d' utiliser la méthode de la question III.4 (sur les qbits 1 à 6) ; pour corriger toute erreur de type Z_k , il suffit d'utiliser la méthode de la question III.4 (sur les qbits 7, 8). En enchainant les deux circuits toutes les erreurs de type X_k, Z_k sont donc corrigées (voir le circuit de la figure 4).
En fait , comme $Y_k = iZ_kX_k$, sur un état de la forme $Y_k |\psi\rangle = iZ_kX_k |\psi\rangle$ le circuit correcteur produira

$$(Z_kX_k) \cdot (iZ_kX_k |\psi\rangle) = i |\psi\rangle$$

i.e. l'état corrigé (au coefficient i près). Cet état est physiquement indiscernable de l'état correct $|\psi\rangle$.
7- Supposons que

$$|\psi\rangle' = (I^p \otimes E \otimes I^{9-p-1}) |\psi\rangle$$

où $E \in \mathbb{M}_{2,2}(\mathbb{C})$. On a vu à la question II.5 qu'il existe des coefficients $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ tel que

$$E = \alpha I + \beta X + \gamma Y + \delta Z.$$

L'effet du circuit détecteur-correcteur D sur cet état sera (par linéarité de D) :

$$D \cdot E \cdot |\psi\rangle = \alpha |\psi\rangle + \beta |\psi\rangle + i\gamma |\psi\rangle + \delta |\psi\rangle = \lambda |\psi\rangle$$

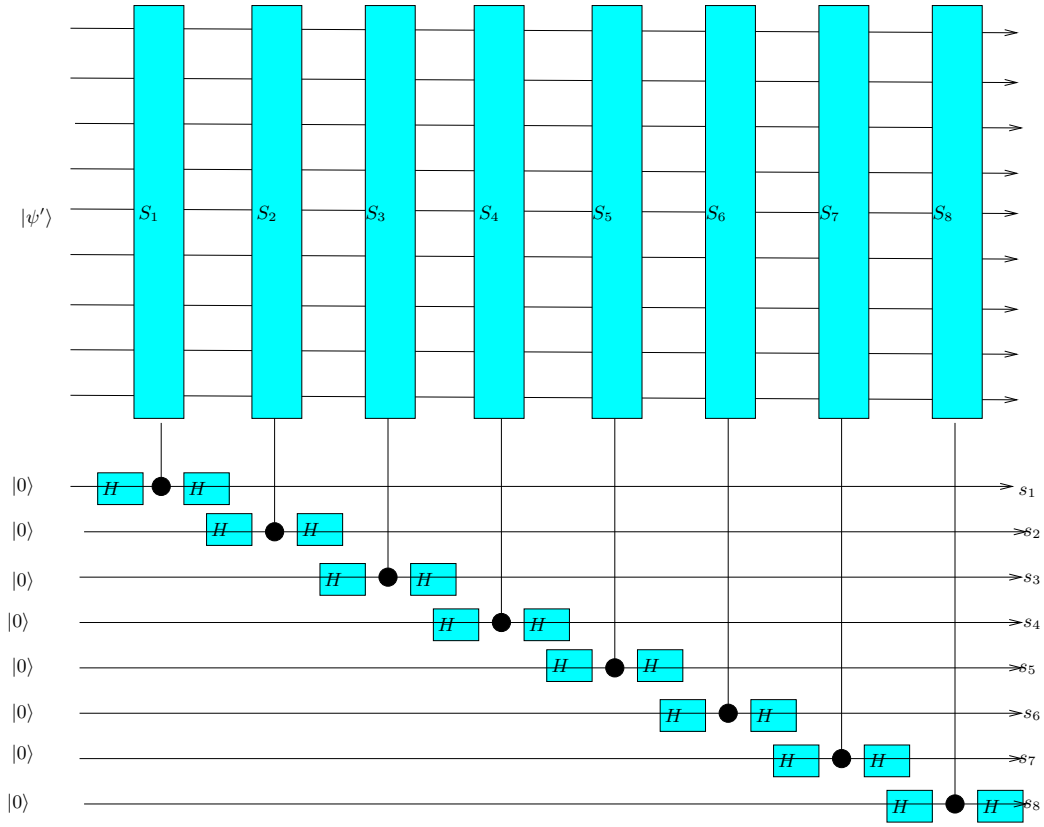

FIGURE 3 – Circuit détecteur de Shor

avec

$$\lambda = \alpha + \beta + i\gamma + \delta.$$

l' état corrigé $\lambda \cdot |\psi\rangle$ est donc physiquement indiscernable de l'état correct $|\psi\rangle$.

Partie V

Construction d'un code quantique à partir d'un code classique.

Nous appliquons ici la méthode CSS (Calderbank-Shor-Steane) au code de Hamming de la partie I ; nous obtenons ainsi un code quantique sur 7 qbits qui corrige *toute* erreur commise sur un seul qbit.
On considère les 3 éléments du groupe $\mathbb{P}_7$ obtenus à partir des 3 lignes de la

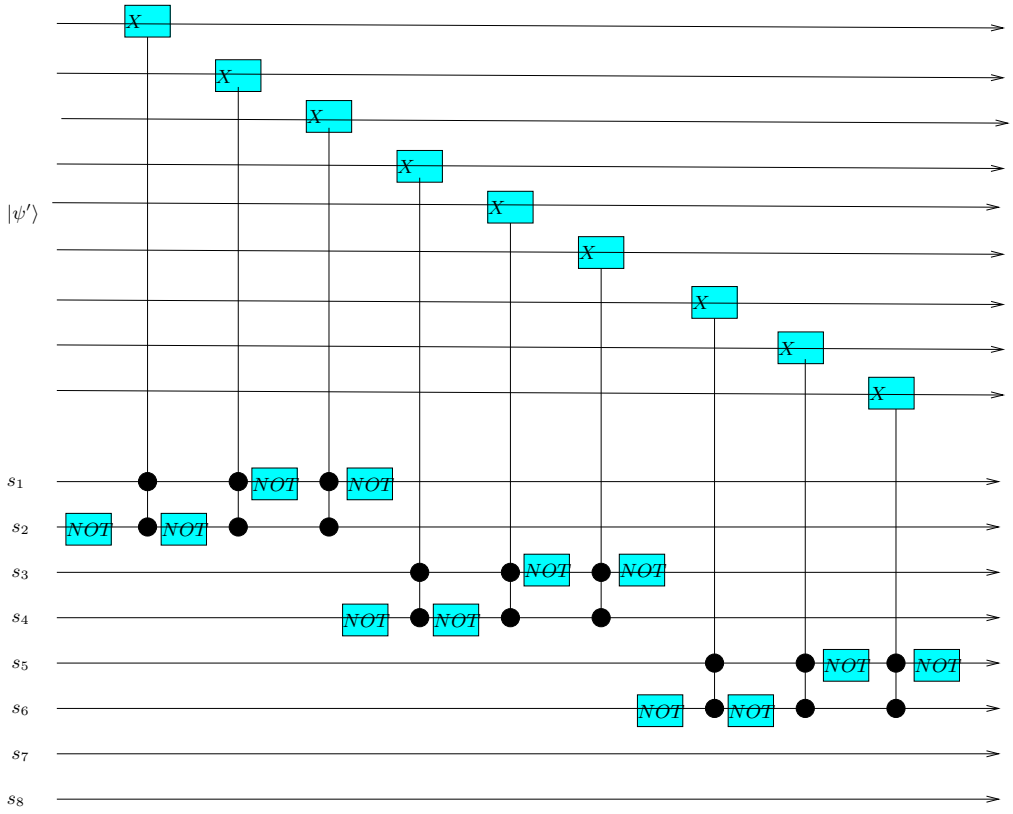

FIGURE 4 – Circuit correcteur de Shor : les flips

matrice H de la partie I :

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

$$S_1 := X_2X_3X_4X_5, \quad S_2 := X_1X_3X_4X_6, \quad S_3 := X_1X_2X_4X_7,$$

puis, en faisant de même avec l'opérateur Z (au lieu de X)

$$S_4 := Z_2Z_3Z_4Z_5, \quad S_5 := Z_1Z_3Z_4Z_6, \quad S_6 := Z_1Z_2Z_4Z_7,$$

1- Il suffit de vérifier que ces transformations commutent deux à deux.

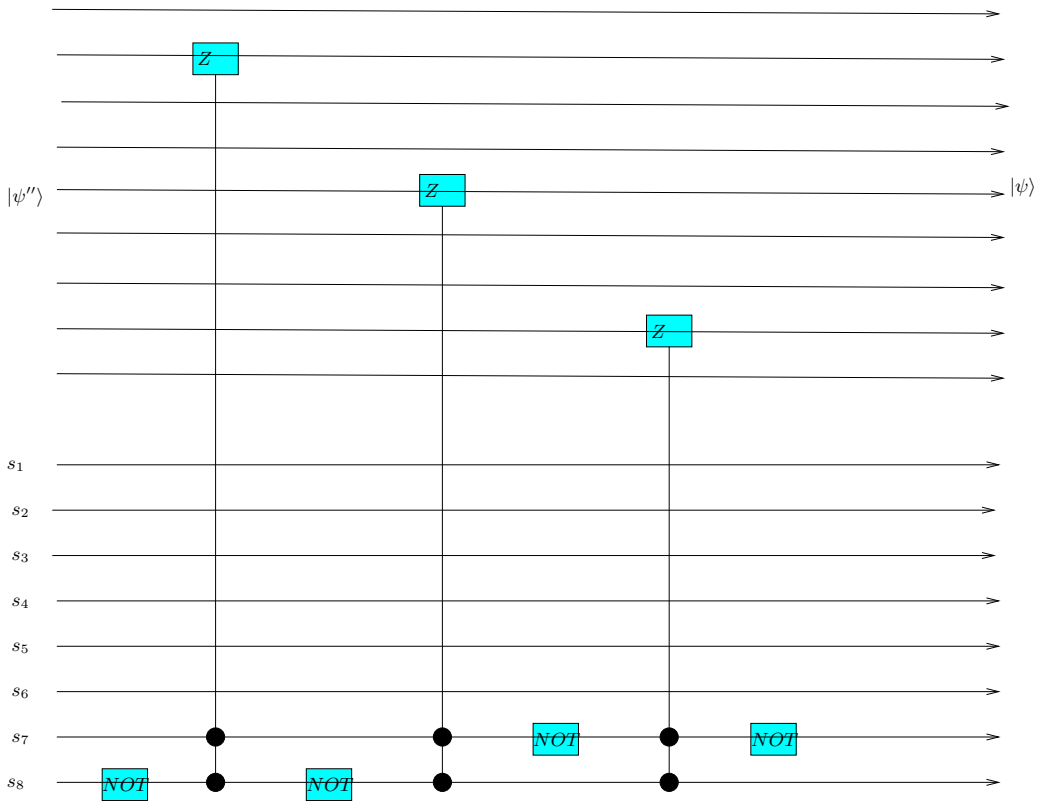

FIGURE 5 – Circuit correcteur de Shor : les phases-flips

2- 2.1 Soit $|u\rangle$ un vecteur et

$$|\bar{u}\rangle := (\prod_{j=1}^{6}(I + S_j)) \cdot |u\rangle$$

Soit $\ell \in [1, 6]$. Par QV.1, S_ℓ commute avec tous les S_j et aussi avec I. Donc

$$\begin{aligned}
S_\ell\,|\bar{u}\rangle &= S_\ell(\textstyle\prod_{j=1}^{6}(I + S_j)) \cdot |u\rangle \\
&= S_\ell(I + S_\ell)(\textstyle\prod_{j\neq\ell}(I + S_j)) \cdot |u\rangle \\
&= (I + S_\ell)(\textstyle\prod_{j\neq\ell}(I + S_j)) \cdot |u\rangle \qquad \text{car } S_\ell(I + S_\ell) = S_\ell + S_\ell^2 = I + S_\ell \\
&= (\textstyle\prod_{j=1}^{6}(I + S_j)) \cdot |u\rangle \\
&= |\bar{u}\rangle
\end{aligned}$$

2.2 Posons

$$|v_0\rangle = (\prod_{j=1}^{6}(I+S_j))\cdot\left|0^7\right\rangle, \;\; |v_1\rangle = (\prod_{j=1}^{6}(I+S_j))\cdot\left|1^7\right\rangle$$

Remarquons que $\left|0^7\right\rangle, \left|1^7\right\rangle$ sont invariants par S_4, S_5, S_6 Donc

$$|v_0\rangle := (\prod_{j=1}^{3}(I+S_j))\cdot\left|0^7\right\rangle, \;\; |v_1\rangle := (\prod_{j=1}^{3}(I+S_j))\cdot\left|1^7\right\rangle$$

On calcule :

$$\prod_{j=1}^{3}(I+S_j) = 1 + X_1X_2X_3X_4(X_5X_6X_7 + X_5X_6 + X_6X_7 + X_5X_7)$$

D' où

$$|v_0\rangle = 8(\left|0^7\right\rangle + \left|1^4\right\rangle[|111\rangle + |110\rangle + |011\rangle + |101\rangle])$$
$$|v_1\rangle = 8(\left|1^7\right\rangle + \left|0^4\right\rangle[|000\rangle + |001\rangle + |100\rangle + |010\rangle])$$

L'image de ces deux vecteurs par la projection orthogonale sur le sous-espace engendré par $|1111110\rangle, |0000001\rangle$ sont les deux vecteurs $|1111110\rangle, |0000001\rangle$, qui sont linéairement indépendants. Donc le sous-espace des vecteurs invariants par les S_j ($j \in [1,6]$) est de dimension ≥ 2 ; donc il possède au moins deux vecteurs orthogonaux unitaires $|\bar{0}\rangle, |\bar{1}\rangle$.
3- Pour tout vecteur-colonne $u \in F_2^7$, et $P \in \mathbb{P}$ on note

$$P^u := \prod_{k=1}^{7} P_k^{u_k}, \;\; H\cdot u = \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix}$$

4- Notation : écrivons chaque S_j sous la forme :

$$S_j = S_{j,1}\cdots S_{j,k}\cdots S_{j,7}$$

Le choix des S_j est calqué sur la ligne j de la matrice H i.e.

$$S_{j,k} = X_k \text{ si } h_{j,k} = 1, \;\; S_{j,k} = I \text{ si } h_{j,k} = 0,$$

Pour $j \in [1,3]$ comme chaque X_k anti-commute avec Z_k, on a :

$$S_{j,k}Z_k^{u_k}S_{j,k}^{-1} = (-1)^{h_{j,k}\cdot u_k}Z_k^{u_k}. \tag{8}$$

En effet :
- si $u_k = 0$, $Z_k^{u_k} = I$ qui commute avec $S_{j,k}$
- si $h_{j,k} = 0$, $S_{j,k} = I$ qui commute avec $Z_k^{u_k}$
- si $h_{j,k} = 1$ et $u_k = 1$, $S_{j,k} Z_k^{u_k} S_{j,k}^{-1} = X_k Z_k X_k^{-1} = (-1) Z_k$

Dans le produit $S_j Z^u S_j^{-1} = (\prod_{k=1}^7 S_{j,k})(\prod_{k=1}^7 Z_k^{u_k})(\prod_{k=1}^7 S_{j,k}^{-1})$, les transformations agissant sur le k-ieme q-bit commutent avec les transformations agissant sur le ℓ-ieme q-bit (pour $k \neq \ell$), donc

$$\begin{aligned} S_j Z^u S_j^{-1} &= (\prod_{k=1}^7 S_{j,k})(\prod_{k=1}^7 Z_k^{u_k})(\prod_{k=1}^7 S_{j,k}^{-1}) \\ &= \prod_{k=1}^7 (S_{j,k} Z_j^{u_k} S_{j,k}^{-1}) \\ &= \prod_{k=1}^7 (-1)^{h_{j,k} \cdot u_k} \cdot Z_k^{u_k} \qquad \text{par l'équation (8)} \\ &= (-1)^{\sum_{k=1}^7 h_{j,k} \cdot u_k} \cdot Z^u \\ &= (-1)^{s_j} Z^u \end{aligned}$$

Par un raisonnement analogue, en échangenat les rôles de X et de Z dans le raisonnement précédent, on obtient que, pour tout $j \in [1, 3]$:

$$S_{3+j} X^u S_{3+j}^{-1} = (-1)^{s_j} X^u.$$

5- Les tables de syndromes de ce code quantique sont donc :

$\lambda \backslash P$:	I	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_7
λ_1	1	1	-1	-1	-1	-1	1	1
λ_2	1	-1	1	-1	-1	1	-1	1
λ_3	1	-1	-1	1	-1	1	1	-1

$\lambda \backslash P$:	I	X_1	X_2	X_3	X_4	X_5	X_6	X_7
λ_4	1	1	-1	-1	-1	-1	1	1
λ_5	1	-1	1	-1	-1	1	-1	1
λ_6	1	-1	-1	1	-1	1	1	-1

6- Par la même méthode que pour les parties III et IV, on obtient un circuit qui détecte les erreurs et calcule les syndromes : voir la figure 6. et un circuit qui, prenant en entrée le vecteur erroné et le syndrome, rétablit le vecteur correct (à un facteur i près dans le cas d'une erreur de type Y_k), voir la figure 7 pour la correction des erreurs de type Z (phase-flips) et la figure 8 pour la correction des erreurs de type X (flips).

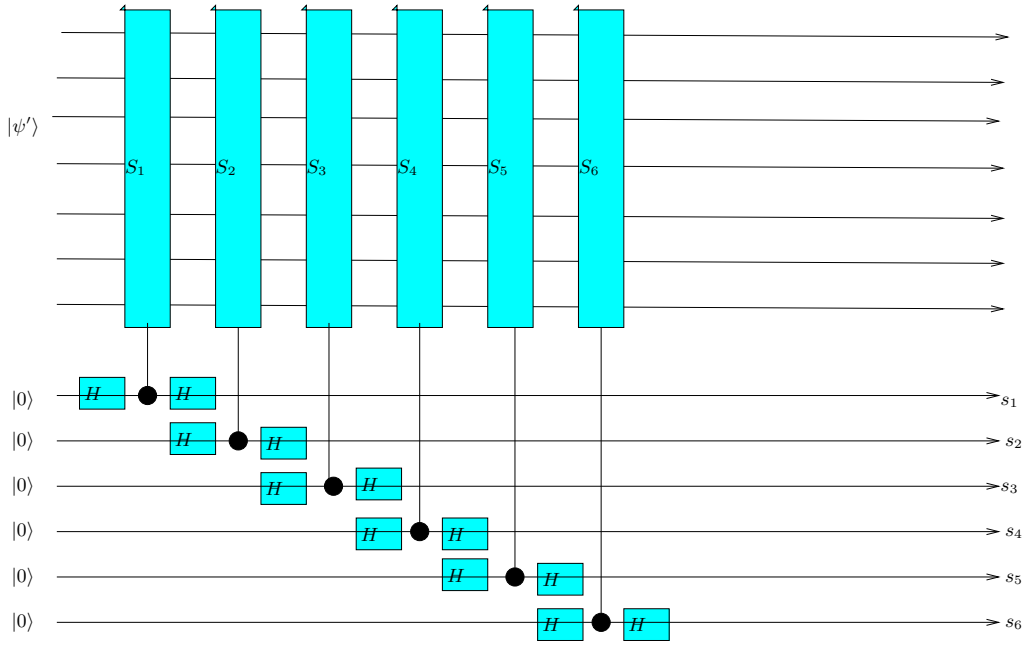

FIGURE 6 – Circuit détecteur, code CSS

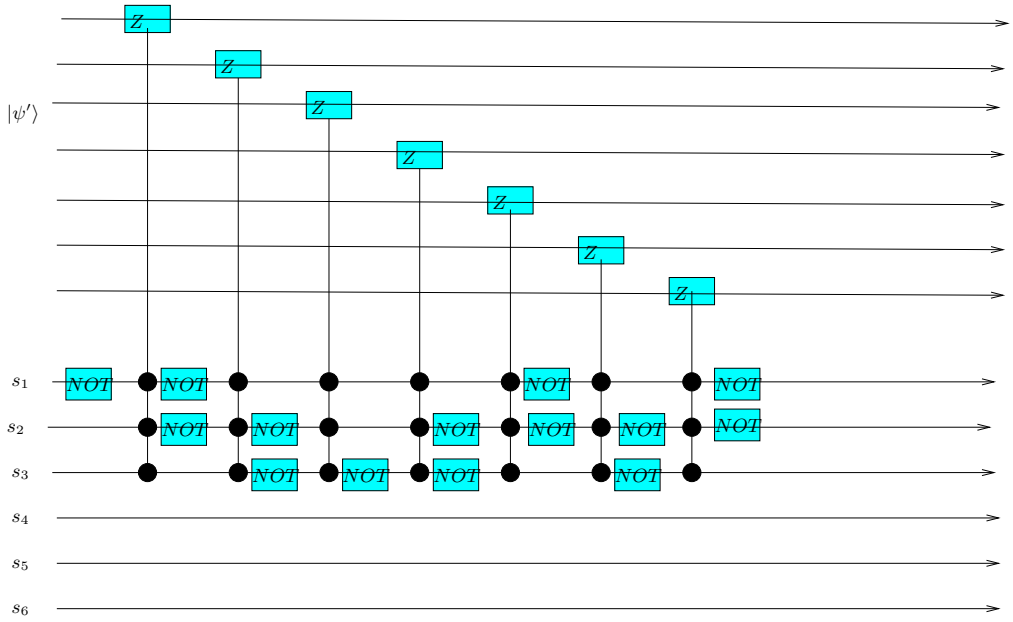

FIGURE 7 – Circuit correcteur CSS : les phases-flips

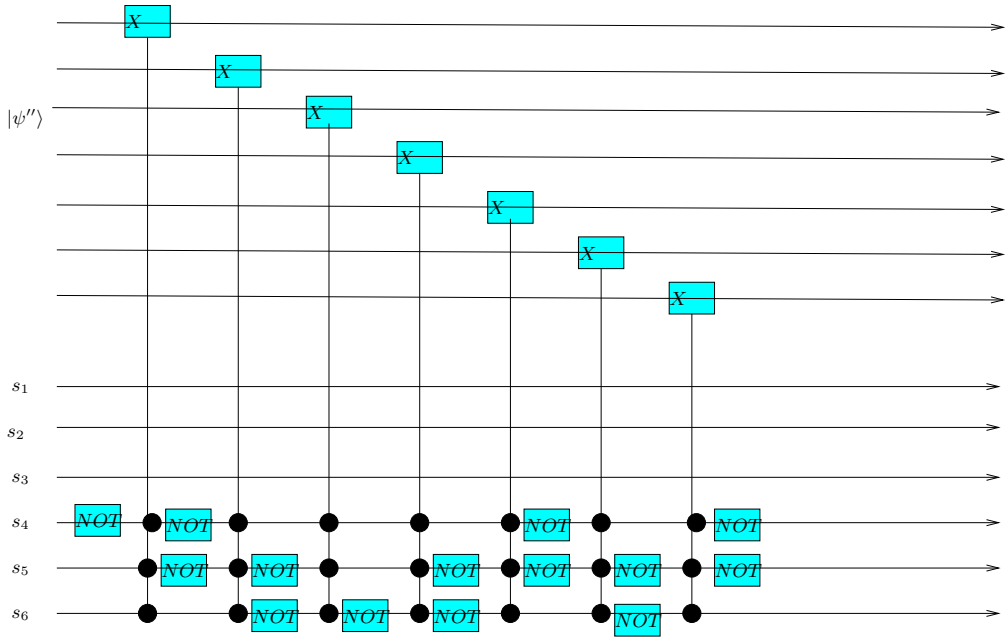

FIGURE 8 – Circuit correcteur CSS : les flips