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

Information Quantique

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

Indications : Chaque partie dépend des parties précédentes.
On peut *admettre* une question (voire même toute une partie) et utiliser les résultats de cette question (ou partie) dans la suite du problème.
Tous moyens d'investigation autorisés. Rédaction finale *individuelle*. Version amendée (le 02/05/2016) grâce aux remarques des étudiants.

Partie I

Un code linéaire classique.

Dans cette première partie, on étudie un code linéaire autocorrecteur, au sens classique du terme. Le *code de Hamming* est défini par la matrice (4,7) suivante :

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

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- Ecrire un système de 3 équations linéaires sur les variables $y_1, \ldots, y_7$ qui expriment que le vecteur $y \in F_2^7$ est dans le sous-espace C de F_2^7 engendré par les lignes de G.
2- En déduire une matrice H, de dimension $(3, 7)$, telle que : pour tout $y \in F_2^7$,

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

On appelle *syndrome* d'une classe $y + C$ le vecteur colonne

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

3- Vérifier que

$$\mathrm{Syn} : y + C \mapsto H \cdot {}^t y$$

est une bijection de F_2^7/C dans l'espace F_2^3 (vu comme l'ensemble des vecteurs-colonnes de dimension 3).
On appelle *poids* du vecteur $u \in F_2^n$ l' entier

$$\mathrm{wt(u)} := \mathrm{Card}(\{\mathrm{k} \in [1, \mathrm{n}] \mid \mathrm{u_k} = 1\}).$$

Les vecteurs $e \in F_2^7$, de poids ≤ 1 sont le vecteur nul $\overrightarrow{0}$ et les vecteurs e_k ($k \in [1, 7]$) où e_k a toutes ses composantes nulles, sauf la k-ième.
4- 4.1 Calculer la table des syndromes des vecteurs de poids ≤ 1.

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

4.2 Vérifier que les syndromes des 8 vecteurs de poids ≤ 1 sont tous distincts.
5- Donner une méthode de décodage $\bar{\varphi} : F_2^7 \to F_2^4$ de façon que, pour tout $w \in F_2^4$ et tout vecteur $e \in F_2^7$ de poids ≤ 1 :

$$\bar{\varphi}(\varphi(w) + e) = w.$$

Partie II

Groupes de Pauli.

On note I la matrice identité de dimension 2×2 et on rappelle la définition des matrices de Pauli, traditionnellement notées X, Y, Z :

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

1- Montrer que l'ensemble de matrices $\mathbb{P} := \{c \cdot M \mid c \in \{1, -1, i, -i\},\ M \in \{I, X, Y, Z\}\}$ forme un sous-groupe de $U(2)$ (le groupe unitaire de dimension 2).
2- Vérifier que

$$X^2 = Y^2 = Z^2 = I$$

En déduire que

$$Spec(X) = Spec(Y) = Spec(Z) = \{-1, 1\}.$$

3- Montrer que , pour tous $P, Q \in \mathbb{P}$,

$$P^{-1}QP \in \{1, -1\} \cdot Q$$

4- Montrer que, pour tous $P, Q \in \mathbb{P}$, et tout $|u\rangle$ vecteur propre de Q,

$$P\,|u\rangle \text{ est vecteur propre de } Q.$$

5- Montrer que l'espace vectoriel (sur $\mathbb{C}$) engendré par $\{I, X, Y, Z\}$ est l'espace de toutes les matrices de dimension 2 à coefficients dans $\mathbb{C}$.

On définit $\mathbb{P}_n$ comme l'ensemble des matrices de dimension $2^n \times 2^n$, de la forme :

$$P_1 \otimes \cdots \otimes P_k \otimes \cdots \otimes P_n$$

avec, pour tout $k \in [1, n]$, $P_k \in \mathbb{P}$. En particulier on note

$$X_k := I^{\otimes(k-1)} \otimes X \otimes I^{\otimes(n-k)}, \;\; Y_k := I^{\otimes(k-1)} \otimes Y \otimes I^{\otimes(n-k)}, \;\; Z_k := I^{\otimes(k-1)} \otimes Z \otimes I^{\otimes(n-k)}.$$

6- Montrer que $\mathbb{P}_n$ est un sous-groupe du groupe unitaire de dimension 2^n.
7- Montrer que, pour tous $P, Q \in \mathbb{P}_n$ et tout $|u\rangle$ vecteur propre de Q,

$$P\,|u\rangle \text{ est vecteur propre de } Q.$$

8- Montrer que l'espace vectoriel (sur $\mathbb{C}$) engendré par P_n est l'espace de toutes les matrices de dimension 2^n.

Partie III

Un premier code quantique.

Dans cette partie, on définit un code quantique permettant de corriger les erreurs de type "flip" .
On dit qu'un vecteur $|\psi\rangle \in \mathcal{B}^{\otimes n}$ est affecté par un "flip" sur la k-ième composante, s'il a été remplacé par

$$X_k\,|\psi\rangle\,.$$

On considère les deux éléments du groupe $\mathbb{P}_3$:

$$S_1 := Z_1 \cdot Z_2, \;\; S_2 := Z_2 \cdot Z_3.$$

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

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

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

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

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

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

1- 1.1 Vérifier que $\left|\bar{0}\right\rangle, \left|\bar{1}\right\rangle$ sont des vecteurs unitaires, orthogonaux et invariants par S_1 et par S_2.
1.2 En déduire que $\left|\psi\right\rangle$ est invariant par S_1 et S_2.
1.3 En déduire que $\left|\psi\right\rangle, X_1\left|\psi\right\rangle, X_2\left|\psi\right\rangle, X_3\left|\psi\right\rangle$ sont des vecteurs propres de S_1 et aussi de S_2.

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

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

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

2- Remplir le tableau des syndromes :

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

On considère le circuit quantique suivant (sur 5 qbits).
On note U la transformation unitaire calculée par ce circuit.

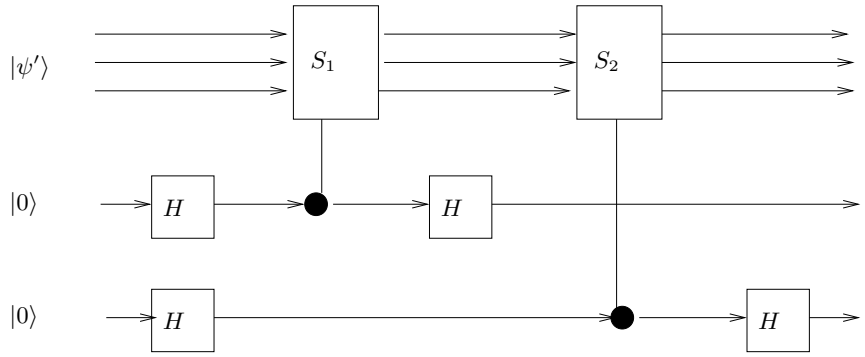

FIGURE 1 – Circuit détectant un flip

3- Montrer que, pour tout état $\left|\psi'\right\rangle$ comportant au plus une erreur, et cette

erreur étant de type flip :

$$U(\left|\psi'\right\rangle \otimes |00\rangle) = \left|\psi'\right\rangle \otimes |s_1, s_2\rangle$$

où $((-1)^{s_1}, (-1)^{s_2})$ est le syndrome de $|\psi'\rangle$.
4- Construire un circuit quantique, avec deux qbits auxiliaires, qui corrige tout état $|\psi'\rangle$ comportant au plus une erreur, et seulement de type flip. Autrement dit : si l'entrée du circuit est $P|\psi\rangle$, avec $P \in \{I, X_1, X_2, X_3\}$, alors la sortie est l'état original $|\psi\rangle$.
Indication : on pourra utiliser les deux q-bits additionnels du circuit comme des qbits auxiliaires et les faire agir sur les qbits de contrôle de portes $\Lambda(X)$ ou $\Lambda^2(X)$.

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 8 éléments du groupe $\mathbb{P}_9$:

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

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

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

$$|\psi\rangle = \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle \tag{2}$$

1- 1.1 Vérifier que $|\bar{0}\rangle, |\bar{1}\rangle$ sont des vecteurs unitaires, orthogonaux et invariants par toutes les transformations S_j ($j \in [1, 8]$).
1.2 En déduire que $|\psi\rangle$ est invariant par toutes les transformations S_j ($j \in [1, 8]$).
1.3 En déduire que, pour tout $k \in [1, 9]$, $|\psi\rangle, X_k|\psi\rangle, Z_k|\psi\rangle, Y_k|\psi\rangle$ 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

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

2- Montrer que le syndrome de l'état $P|\psi\rangle$ ne dépend que de P.

3- Calculer 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										
$\vdots$										
λ_8										

puis la table des syndromes pour les erreurs Z_k, ($k \in [1,9]$).
4- Comment en déduit-on la table des syndromes pour les erreurs Y_k ($k \in [1,9]$) ?
5- Construire un circuit qui "calcule le syndrome" (dans le même sens qu'à la question III.3) de tout état erroné de la forme $P|\psi\rangle$ où $|\psi\rangle$ est de la forme (2) et P est un opérateur I ou X_k ou Y_k ou Z_k ($k \in [1,9]$).
6- Calculer un circuit qui corrige toute erreur de type I, X_k, Y_k, Z_k sur un seul qbit d'un état de la forme (2).
7- Ce circuit corrige-t-il, en fait, *toute* erreur qui ne porte que sur un seul qbit ? i.e. transforme-t-il tout vecteur de la forme $(I^p \otimes E \otimes I^{9-p-1})|\psi\rangle$, pour E transformation linéaire *quelconque*, et $|\psi\rangle$ de la forme (2), en $|\psi\rangle$?

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 matrice H de la partie I :

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

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

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

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

1- Vérifier que $\{I\} \cup \{S_j \mid 1 \leq j \leq 6\}$ *engendre* un sous-groupe abélien de $\mathbb{P}_7$.
2- Montrer qu'il existe un couple de vecteurs unitaires, orthogonaux, $(|\bar{0}\rangle, |\bar{1}\rangle)$,

invariants par toutes les transformations S_j ($j \in [1,6]$).
Indication : on remarquera que tout vecteur de la forme $(\prod_{j=1}^{6}(I+S_j)) \cdot |u\rangle$ est invariant par tous les S_j.

Soit

$$|\psi\rangle = \alpha\,|\bar{0}\rangle + \beta\,|\bar{1}\rangle \tag{3}$$

3- Pour tout vecteur-colonne $u \in F_2^7$, et $P \in \mathbb{P}$ on note

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

4- Montrer que, pour tout $j \in [1,3]$:

$$S_j Z^u S_j^{-1} = (-1)^{s_j} Z^u, \quad S_{3+j} X^u S_{3+j}^{-1} = (-1)^{s_j} X^u.$$

5- Déduire les tables de syndromes de ce code quantique de celle du code de Hamming (q. I.4).
6- Calculer un circuit qui corrige toute erreur de type X_k, Y_k, Z_k sur un seul qbit d'un état de la forme (3).