ENSEIRB-MATMECA
Option second semestre, 2014/2015

Information Quantique

Corrigé de l'examen du 20 Mai 2015

La note finale est min(20, note-ex1+note-ex2+note-ex3).

Exercice 1 (/5 pts)

Théorème de non-clonage.

On veut montrer qu'il n'existe pas de transformation unitaire

$$U : \mathcal{B} \otimes \mathcal{B} \otimes \mathcal{H} \to \mathcal{B} \otimes \mathcal{B} \otimes \mathcal{H}$$

qui permette de *cloner* les états de $\mathcal{B}$ au sens suivant : $\forall \left|\Phi\right\rangle \in \mathcal{B}, \exists \left|d\right\rangle \in \mathcal{H}$

$$U \left|\Phi\right\rangle \otimes \left|b\right\rangle \otimes \left|c\right\rangle = \left|\Phi\right\rangle \otimes \left|\Phi\right\rangle \otimes \left|d\right\rangle \tag{1}$$

Supposons qu'une transformation unitaire U vérifiant (1) existe.
Considérons des états $\left|\Phi\right\rangle, \left|\Psi\right\rangle \in \mathcal{B}$ et $\left|d\right\rangle, \left|d'\right\rangle \in \mathcal{H}$ tels que (1) est vraie ainsi que son analogue (2) :

$$U \left|\Psi\right\rangle \otimes \left|b\right\rangle \otimes \left|c\right\rangle = \left|\Psi\right\rangle \otimes \left|\Psi\right\rangle \otimes \left|d'\right\rangle \tag{2}$$

1- Par définition du produit scalaire dans le produit tensoriel : le produit scalaire de $\Phi \otimes \left|b\right\rangle \otimes \left|c\right\rangle$ par $\Psi \otimes \left|b\right\rangle \otimes \left|c\right\rangle$ est :

$$\begin{aligned} \left\langle c\right| \left\langle b\right| \left\langle \Phi|\Psi\right\rangle \left|b\right\rangle \left|c\right\rangle &= \left\langle \Phi|\Psi\right\rangle \left\langle b|b\right\rangle \left\langle c|c\right\rangle \\ &= \left\langle \Phi|\Psi\right\rangle \text{ puisque } \left|b\right\rangle, \left|c\right\rangle \text{ sont unitaires.} \end{aligned}$$

De même, le produit scalaire de $\Phi \otimes \Phi \otimes \left|d\right\rangle$ par $\Psi \otimes \left|\Psi\right\rangle \otimes \left|d'\right\rangle$ est :

$$\left\langle d\right| \left\langle \Phi\right| \left\langle \Phi|\Psi\right\rangle \left|\Psi\right\rangle \left|d'\right\rangle = \left\langle \Phi|\Psi\right\rangle^2 \left\langle d|d'\right\rangle$$

Mais l'opérateur U est unitaire, i.e. préserve le produit scalaire. Les deux produits calculés ci-dessus sont donc égaux :

$$\left\langle \Phi|\Psi\right\rangle^2 \left\langle d|d'\right\rangle = \left\langle \Phi|\Psi\right\rangle$$

ce qui est équivalent à

$$\left\langle \Phi|\Psi\right\rangle \left(\left\langle \Phi|\Psi\right\rangle \left\langle d|d'\right\rangle - 1\right) = 0$$

2- le produit ci-dessus est nul ssi l' un de ses facteurs est nul i.e.

$$\langle\Phi|\Psi\rangle = 0(\text{ cas 0}) \text{ ou } \langle\Phi|\Psi\rangle \left\langle d|d'\right\rangle = 1(\text{ cas 1}).$$

Dans le cas 0 : $|\Phi\rangle, |\Psi\rangle$ sont orthogonaux.
Dans le cas 1 : par l'inégalité de Cauchy-Schwarz,

$$\begin{aligned} 1 = \langle\Phi|\Psi\rangle \left\langle d|d'\right\rangle &\leq \|\Phi\| \cdot \|\Psi\| \cdot \|d\| \cdot \|d'\| \\ &= 1 \text{ puisque les quatre vecteurs sont unitaires} \end{aligned}$$

Ceci n'est donc possible que si $\langle\Phi|\Psi\rangle = \|\Phi\| \cdot \|\Psi\|$, c'est à dire le cas d'égalité dans l'inégalité de CS. Mais cette égalité n'a lieu que lorsque les vecteurs sont colinéaires. Donc $|\Phi\rangle, |\Psi\rangle$ sont colinéaires.
3- Supposons que ce système réalise la transformation unitaire U. Supposons que U clone un vecteur unitaire $|\Phi\rangle$. L'orthogonal de la droite vect($|\Phi\rangle$) est une droite vect($|\Phi'\rangle$). Par la question 2, le système ne peut cloner que les vecteurs unitaires appartenant à l'ensemble :

$$\text{vect}(|\Phi\rangle) \cup \text{vect}(|\Phi'\rangle)$$

i.e. l'union de *deux* droites vectorielles (restreintes à leurs vecteurs unitaires). Finalement : un sytème quantique ne peut cloner que *au plus deux* droites.

Exercice 2 (/15 pts)

Théorème de non-effacement.

1- Supposons que la transformation unitaire

$$U : \mathcal{B} \otimes \mathcal{B} \to \mathcal{B} \otimes \mathcal{B}$$

et le vecteur $|N\rangle \in \mathcal{B}$ vérifient que, pour tout $|\Phi\rangle \in \mathcal{B}$,

$$U|\Phi\rangle|\Phi\rangle = |\Phi\rangle|N\rangle.$$

Ce serait en particulier vrai pour les vecteurs unitaires $|\Phi\rangle \in \mathcal{B}$.
Mais alors U^{-1} serait une " photocopieuse quantique" i.e. vérifierait la propriété de l'exercice 1 avec $n = \dim(\mathcal{H}) = 0$. Comme il n'en existe pas, $U, |N\rangle$ n'existent pas.
2- Considérons la transformation linéaire $\mathsf{SWAP} : \mathcal{B} \otimes \mathcal{B} \to \mathcal{B} \otimes \mathcal{B}$ définie par, pour tous $(i,j) \in \{0,1\}^2$,

$$|i\rangle|j\rangle \mapsto |j\rangle|i\rangle.$$

Comme l'image de la base orthonormée $\{|i\rangle|j\rangle \mid (i,j) \in \{0,1\}^2\}$ est une famille orthonormée (une permutation de la famille initiale), cette transformation est unitaire. Soit $U : \mathcal{B} \otimes \mathcal{B} \otimes \mathcal{B}$, et $|N\rangle, |A\rangle \in \mathcal{B}$ définis par :

$$U := \mathrm{Id}_{\mathcal{B}} \otimes \mathsf{SWAP}, \quad |N\rangle := |0\rangle, \quad |A\rangle := |0\rangle.$$

Pour tous $|\Phi\rangle \in \mathcal{B}$,

$$U|\Phi\rangle|\Phi\rangle|0\rangle = |\Phi\rangle|0\rangle|\Phi\rangle,$$

La transformation U a donc la propriété recquise.
On suppose que la transformation unitaire U et les vecteurs unitaires $|N\rangle \in \mathcal{B}, |A\rangle \in \mathcal{H}$ vérifient la propriété

$$U|\Phi\rangle|\Phi\rangle|A\rangle = |\Phi\rangle|N\rangle|A'\rangle. \tag{3}$$

Nous trouverons, à la qu. 8, une transformation unitaire $D : \mathcal{B} \otimes \mathcal{H} \to \mathcal{B} \otimes \mathcal{H}$ telle que, pour tout $|\Phi\rangle \in \mathcal{B}$

$$(\mathrm{Id}_{\mathcal{B}} \otimes D) \circ U|\Phi\rangle|\Phi\rangle|A\rangle = |\Phi\rangle|\Phi\rangle|A\rangle \tag{4}$$

Notons $|A_0\rangle, |A_1\rangle$ les vecteurs de $\mathcal{H}$ tels que

$$U|0\rangle|0\rangle|A\rangle = |0\rangle|N\rangle|A_0\rangle \text{ et } U|1\rangle|1\rangle|A\rangle = |1\rangle|N\rangle|A_1\rangle.$$

Soit $|\Phi\rangle \in \mathcal{B}$. Il est donc de la forme $\alpha|0\rangle + \beta|1\rangle$ pour des coefficients $\alpha, \beta \in \mathbb{C}$. Notons $|A(\alpha,\beta)\rangle$ un vecteur de $\mathcal{H}$ tel que

$$U|\Phi\rangle|\Phi\rangle|A\rangle = |\Phi\rangle|N\rangle|A(\alpha,\beta)\rangle. \tag{5}$$

3- Considérons le vecteur

$$V(\alpha,\beta) := U(\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)|A\rangle$$

Par bilinéarité de l'application $(|u\rangle, |u\rangle) \mapsto U|u\rangle|u\rangle|A\rangle$ on a :

$$V(\alpha,\beta) = \alpha^2|0\rangle|N\rangle|A_0\rangle + \beta^2|1\rangle|N\rangle|A_1\rangle + \alpha\beta U|0\rangle|1\rangle|A\rangle + \beta\alpha U|1\rangle|0\rangle|A\rangle.$$

Posons

$$|F\rangle = U(\frac{1}{\sqrt{2}}[|0\rangle|1\rangle|A\rangle + |1\rangle|0\rangle|A\rangle])$$

Comme le vecteur $[|0\rangle|1\rangle|A\rangle + |1\rangle|0\rangle|A\rangle]$ a un carré de norme égal à deux (somme de deux vecteurs unitaires orthogonaux), et comme U préserve la norme,

$$\|F\| = 1.$$

On obtient alors

$$V(\alpha,\beta) = \alpha^2 \left|0\right\rangle \left|N\right\rangle \left|A_0\right\rangle + \beta^2 \left|1\right\rangle \left|N\right\rangle \left|A_1\right\rangle + \sqrt{2}\alpha\beta \left|F\right\rangle .$$

D'autre part, en appliquant l'identité (5) on obtient :

$$\begin{aligned} V(\alpha,\beta) &= (\alpha \left|0\right\rangle + \beta \left|1\right\rangle) \left|N\right\rangle \left|A(\alpha,\beta)\right\rangle \\ &= \alpha \left|0\right\rangle \left|N\right\rangle \left|A(\alpha,\beta)\right\rangle + \beta \left|1\right\rangle \left|N\right\rangle \left|A(\alpha,\beta)\right\rangle \end{aligned}$$

Les deux expressions trouvées pour $V(\alpha,\beta)$ doivent être égales i.e.

$$\alpha^2 \left|0\right\rangle \left|N\right\rangle \left|A_0\right\rangle + \beta^2 \left|1\right\rangle \left|N\right\rangle \left|A_1\right\rangle + \sqrt{2}\alpha\beta \left|F\right\rangle = \alpha \left|0\right\rangle \left|N\right\rangle \left|A(\alpha,\beta)\right\rangle + \beta \left|1\right\rangle \left|N\right\rangle \left|A(\alpha,\beta)\right\rangle \tag{6}$$

4- Remarquons tout d'abord que l'égalité (5) de l'énoncé définit un vecteur $\left|A(\alpha,\beta)\right\rangle$ unique lorsque $(\alpha,\beta) \neq (0,0)$. Choisissons

$$\left|A(0,0)\right\rangle = \overrightarrow{0} \tag{7}$$

attention : c'est le vecteur *nul*, de norme 0 ; ce n'est pas le vecteur $\left|0\right\rangle$, qui est unitaire.
Les sous-espaces $\mathrm{vect}(\left|0\right\rangle \left|N\right\rangle) \otimes \mathcal{H}$ et $\mathrm{vect}(\left|1\right\rangle \left|N\right\rangle) \otimes \mathcal{H}$ sont orthogonaux. Notons pr_0 la projection orthogonale

$$\mathrm{vect}(\left|0\right\rangle \left|N\right\rangle) \otimes \mathcal{H} \oplus \mathrm{vect}(\left|1\right\rangle \left|N\right\rangle) \otimes \mathcal{H} \to \mathrm{vect}(\left|0\right\rangle \left|N\right\rangle) \otimes \mathcal{H},$$

et pr_1 la projection orthogonale de même domaine, mais d'image $\mathrm{vect}(\left|1\right\rangle \left|N\right\rangle) \otimes \mathcal{H}$.
L'égalité (6) implique que les images par pr_0 (resp. pr_1) des deux membres sont égales i.e., pour tous $(\alpha,\beta) \in \mathbb{C}^2$

$$\begin{aligned} \alpha^2 \left|0\right\rangle \left|N\right\rangle \left|A_0\right\rangle + \sqrt{2}\alpha\beta \mathrm{pr}_0 \left|F\right\rangle &= \alpha \left|0\right\rangle \left|N\right\rangle \left|A(\alpha,\beta)\right\rangle & (8) \\ \beta^2 \left|1\right\rangle \left|N\right\rangle \left|A_1\right\rangle + \sqrt{2}\alpha\beta \mathrm{pr}_1 \left|F\right\rangle &= \beta \left|1\right\rangle \left|N\right\rangle \left|A(\alpha,\beta)\right\rangle & (9) \end{aligned}$$

En divisant (8) par α on voit que, si $\alpha \neq 0$:

$$\alpha \left|0\right\rangle \left|N\right\rangle \left|A_0\right\rangle + \sqrt{2}\beta \mathrm{pr}_0 \left|F\right\rangle = \left|0\right\rangle \left|N\right\rangle \left|A(\alpha,\beta)\right\rangle \tag{10}$$

Si $\beta \neq 0$ on a aussi (en divisant (9) par β) :

$$\beta \left|1\right\rangle \left|N\right\rangle \left|A_1\right\rangle + \sqrt{2}\alpha \mathrm{pr}_1 \left|F\right\rangle = \left|1\right\rangle \left|N\right\rangle \left|A(\alpha,\beta)\right\rangle \tag{11}$$

ce qui montre que la fonction $(\alpha,\beta) \mapsto \left|A(\alpha,\beta)\right\rangle$ est continue en $(0,\beta)$ (pour $\beta \neq 0$). En utilisant la formule (10) et en passant à la limite lorsque α tend

vers 0, on obtient, par continuité de $|A(*,*)\rangle$ en $(0,\beta)$, que, si $\alpha = 0$ et $\beta \neq 0$, la formule (10) reste valide. Mais la formule (10) est aussi vraie pour $(\alpha,\beta) = (0,0)$, par le choix (7). Finalement, la formule (10) est toujours valide :

$$\forall \alpha,\beta \in \mathbb{C}, \alpha\,|0\rangle\,|N\rangle\,|A_0\rangle + \sqrt{2}\beta \mathrm{pr}_0\,|F\rangle = |0\rangle\,|N\rangle\,|A(\alpha,\beta)\rangle \qquad (12)$$

Par des arguments analogues on obtient aussi :

$$\forall \alpha,\beta \in \mathbb{C}, \beta\,|1\rangle\,|N\rangle\,|A_1\rangle + \sqrt{2}\alpha \mathrm{pr}_1\,|F\rangle = |1\rangle\,|N\rangle\,|A(\alpha,\beta)\rangle \qquad (13)$$

Notons $H : \mathcal{H} \to \mathrm{vect}(|0\rangle\,|N\rangle) \otimes \mathcal{H}$ l'isomorphisme :

$$|u\rangle \mapsto |0\rangle\,|N\rangle\,|u\rangle$$

L'application $(\alpha,\beta) \mapsto |A(\alpha,\beta)\rangle$ est la composée de

$$(\alpha,\beta) \mapsto |0\rangle\,|N\rangle\,|A(\alpha,\beta)\rangle$$

qui est linéaire selon la formule (12) et de l'application H^{-1} qui est linéaire. Donc elle est linéaire.
5- Par la formule (10) et le choix (7) :

$$|A(\alpha,0)\rangle = \alpha\,|A_0\rangle$$

et par la formule (11) et le choix (7) :

$$|A(0,\beta)\rangle = \beta\,|A_1\rangle\,.$$

Par linéarité de $A(*,*)$ (qu. 4) on en conclut que, pour tout $(\alpha,\beta) \in \mathbb{C}^2$,

$$|A(\alpha,\beta)\rangle = \alpha\,|A_0\rangle + \beta\,|A_1\rangle\,.$$

6- En prenant $\alpha = 0, \beta = 1$ dans (12) on obtient :

$$\mathrm{pr}_0\,|F\rangle = \frac{1}{\sqrt{2}}\,|0\rangle\,|N\rangle\,|A_1\rangle\,.$$

En prenant $\alpha = 1, \beta = 0$ dans (13) on obtient :

$$\mathrm{pr}_1\,|F\rangle = \frac{1}{\sqrt{2}}\,|1\rangle\,|N\rangle\,|A_0\rangle$$

d'où $|F\rangle = \frac{1}{\sqrt{2}}[|0\rangle\,|N\rangle\,|A_1\rangle + |1\rangle\,|N\rangle\,|A_0\rangle]$.
7- Comme $|0\rangle\,|0\rangle\,|A\rangle$ est unitaire, son image par U est unitaire, mais comme

$|0\rangle, |N\rangle$ sont unitaires, il faut que $\|A_0\| = 1$. De même il faut que $\|A_1\| = 1$. Tout vecteur unitaire $|\Phi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathcal{B}$, a une image par U qui est encore unitaire i.e.

$$\|A(\alpha, \beta)\| = 1.$$

Or

$$\|A(\alpha, \beta)\|^2 = |\alpha|^2 + |\beta|^2 + 2\mathcal{R}(\bar{\alpha}\beta)\langle A_0|A_1\rangle$$

Donc, pour des α, β tels que $|\alpha|^2 + |\beta|^2 = 1$, on a :

$$1 = 1 + 2\mathcal{R}(\bar{\alpha}\beta)\langle A_0|A_1\rangle$$

donc $\langle A_0|A_1\rangle = 0$. On en conclut que $(|A_0\rangle, |A_1\rangle)$ est une famille orthonormée.

8- Considérons l'application linéaire $D_0 : \text{vect}(|N\rangle|A_0\rangle, |N\rangle|A_1\rangle) \to \text{vect}(|0\rangle|A\rangle, |1\rangle|A\rangle)$ qui envoie $(|N\rangle|A_0\rangle, |N\rangle|A_1\rangle)$ sur $(|0\rangle|A\rangle, |1\rangle|A\rangle)$. Cette transformation existe car ces deux familles sont libres. Elle est unitaire car ces deux familles sont orthonormées. D_0 est prolongeable en une transformation unitaire $D : \mathcal{B} \otimes \mathcal{H} \to \mathcal{B} \otimes \mathcal{H}$. Comme

$$D|N\rangle(\alpha|A_0\rangle + \beta|A_1\rangle) = \alpha|0\rangle|A\rangle + \beta|1\rangle|A\rangle$$

on a bien

$$\begin{array}{rcl} |\Phi\rangle|\Phi\rangle|A\rangle & \overset{U}{\mapsto} & |\Phi\rangle[|N\rangle(\alpha|A_0\rangle + \beta|A_1\rangle)] \\ & \overset{\text{Id}\otimes D}{\mapsto} & |\Phi\rangle[\alpha|0\rangle|A\rangle + \beta|1\rangle|A\rangle] \\ & = & |\Phi\rangle|\Phi\rangle|A\rangle. \end{array}$$

ce qui établit la propriété (4).

9- Remarquons que la transformation D construite à la question 8 est telle que, les vecteurs *de la forme* $|\Phi\rangle|\Phi\rangle|A\rangle$ (autrement dit : " ceux qui sont des clones") sont des points fixes de $(\text{Id}_{\mathcal{B}} \otimes D) \circ U$.

Considérons la transformation U définie par : $\forall|\Phi_0\rangle \in \mathcal{B}, \forall|\Phi_1\rangle \in \mathcal{B}, \forall|\Psi\rangle \in \mathcal{H}$,

$$U|\Phi_0\rangle|\Phi_1\rangle|\Psi\rangle = |\Phi_1\rangle|\Phi_0\rangle|\Psi\rangle.$$

Comme $U|0\rangle|1\rangle|\Psi\rangle \notin |0\rangle \otimes \mathcal{B} \otimes \mathcal{H}$, ce vecteur ne peut être dans l'image de $(\text{Id}_{\mathcal{B}} \otimes D)$ pour aucune application linéaire $D : \mathcal{B} \otimes \mathcal{H} \to \mathcal{B} \otimes \mathcal{H}$.

Exercice 3(/15 pts)
Cryptographie quantique.

1- Nous présentons dans un tableau toutes les possibilités (i.e. les événements qui ont une probabilité non-nulle de survenir).

x	$qbitA$	y	B_B	μ_B	p	b
0	$\|\uparrow\rangle$	0	$\oplus$	$\|\uparrow\rangle$	$\frac{1}{4}$	0
0	$\|\uparrow\rangle$	1	$\otimes$	$\|\nearrow\rangle$	$\frac{1}{8}$	0
–	–	–	–	$-\|\searrow\rangle$	$\frac{1}{8}$	1
1	$\|\nearrow\rangle$	0	$\oplus$	$\|\uparrow\rangle$	$\frac{1}{8}$	0
–	–	–	–	$\|\rightarrow\rangle$	$\frac{1}{8}$	1
1	$\|\nearrow\rangle$	1	$\otimes$	$\|\nearrow\rangle$	$\frac{1}{4}$	0

Un tiret indique que le contenu d'une cellule est identique à celui de la case au-dessus ; p est la probabilité que ce cas de figure ait lieu : chaque événement $\{x = \alpha, y = \beta\}$ a une probabilité $\frac{1}{4}$ de survenir et, lorsque le qbit de A n'est pas un vecteur de la base de B, chaque résultat de mesure a une chance sur deux de sortir.
Le cas $b = 1$ est décrit aux lignes 3 et 5. Dans le cas de la ligne 3 : $x = 0, y = 1$; dans le cas de la ligne 5 : $x = 1, y = 0$.
2- Solution 1 : Bob publie les indices $i_1, \ldots, i_j, \ldots, i_\ell$ pour lesquels $b = 1$. Ils définissent la clé commune comme :

$$C = x_{i_1} \ldots x_{i_j} \ldots x_{i_\ell} = (1 - y_{i_1}) \ldots (1 - y_{i_j}) \ldots (1 - y_{i_\ell}).$$

Solution 2 : variante obtenue en échangeant x et y dans la solution 1.
Dans la suite du corrigé nous supposons que A,B choisissent la sol. 1.
3- Comme $\Pr(b = 1) = \frac{1}{4}$ la longueur de C est, en moyenne de $n/4$.
4- Supposons que $x = 0$, $B_E = \otimes$, $\mu_E = |\nearrow\rangle$, Eve applique sa stratégie, $y = 0$ et B obtient $\mu_B = |\rightarrow\rangle$.
4.1 Par définition du comportement de B dans le protocole $b = 1$.
4.2 On voit que $x = 0 = y$: il n' est pas vrai que $x \neq y$. Ce fait est dû à l'intervention de E, tandis que la question 1 portait sur le fonctionnement du protocole *en l'absence* de E.
Cette remarque ne contredit donc pas la réponse à la question 1.
4.3 Cette interception par E peut être détectée par A et B : B peut, par exemple, publier ses valeurs de y et de b. Alice publier sa valeur de x. Tous deux savent alors que E est intervenue puisque, selon la qu.1, en l'absence de E, $b = 1 \Rightarrow x \neq y$.
4.4 Sans publication par A de son bit, E *ne peut pas être sûre* de la valeur du

qbit de A : les deux valeurs $|\uparrow\rangle, |\nearrow\rangle$ peuvent aboutir au résultat de mesure $|\nearrow\rangle$ lorsque E utilise la base $\otimes$.
5- Supposons que $x = 0$, $B_E = \otimes$, $\mu_E = |\searrow\rangle$, Eve applique sa stratégie et $y = 0$.
5.1 Par définition du comportement de B dans le protocole, $b = 0$.
5.2 Même si A et B publient *toutes* leurs données (x, y, μ_B), le résultat $\mu_B = |\uparrow\rangle$ est compatible avec le fonctionnement du protocole sans Ève. Donc E *ne peut pas* être détecté par A,B.
5.3 Eve connaît le bit x de A, par le raisonnement suivant :
si A avait envoyé $|\nearrow\rangle$ alors, comme ce vecteur est un vecteur de la base $\otimes$, E aurait mesuré (presque sûrement) $|\nearrow\rangle$; or E a mesuré $|\searrow\rangle$; A ne peut donc avoir envoyé que $|\uparrow\rangle$, donc $x = 0$.
6- 6.1 Un protocole de vérification pour A et B :
- si $b = 0$: A et B ne font rien (nous verrons plus bas qu'en fait, dans ce cas, E est indétectable)
- si $b = 1$: B publie son bit y et A publie son bit x ; s'ils constatent que $x = y$, ils en déduisent que E les espionne et ils abandonnent leur clé C ; sinon ils maintiennent la clé C (en enlevant le bit dans la position qui vient d'être vérifiée puisque ce bit est maintenant connu de tous).
6.2 Voici tous les cas de figure :

x	$qbitA$	B_E	μ_E	$qbitE$	y	B_B	μ_B	b	p
0	$\|\uparrow\rangle$	$\oplus$	$\|\uparrow\rangle$	$\|\uparrow\rangle$	0	$\oplus$	$\|\uparrow\rangle$	0	$\frac{1}{8}$
–	–	–	–	–	1	$\otimes$	$\|\uparrow\rangle$	0	$\frac{1}{16}$
–	–	–	–	–	1	–	$-\|\searrow\rangle$	1	$\frac{1}{16}$
–	–	$\otimes$	$\|\nearrow\rangle$	$\|\nearrow\rangle$	0	$\oplus$	$\|\uparrow\rangle$	0	$\frac{1}{32}$
–	–	–	–	–	0	–	$\|\rightarrow\rangle$	1	$\frac{1}{32}$
–	–	–	–	–	1	$\otimes$	$-\|\searrow\rangle$	0	$\frac{1}{16}$
–	–	–	$-\|\searrow\rangle$	$\|\uparrow\rangle$	0	$\oplus$	$\|\uparrow\rangle$	0	$\frac{1}{16}$
–	–	–	–	–	1	$\otimes$	$\|\nearrow\rangle$	0	$\frac{1}{32}$
–	–	–	–	–	1	–	$-\|\searrow\rangle$	1	$\frac{1}{32}$
1	$\|\nearrow\rangle$	$\oplus$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$	0	$\oplus$	$\|\rightarrow\rangle$	1	$\frac{1}{32}$
–	–	–	–	–	0	$\oplus$	$\|\uparrow\rangle$	0	$\frac{1}{32}$
–	–	–	–	$\|\uparrow\rangle$	1	$\otimes$	$\|\nearrow\rangle$	0	$\frac{1}{16}$
–	–	–	$\|\uparrow\rangle$	$\|\uparrow\rangle$	0	$\oplus$	$\|\uparrow\rangle$	0	$\frac{1}{16}$
–	–	–	–	–	1	$\otimes$	$-\|\searrow\rangle$	1	$\frac{1}{32}$
–	–	–	–	–	1	–	$\|\nearrow\rangle$	0	$\frac{1}{32}$
–	–	$\otimes$	$\|\nearrow\rangle$	$\|\nearrow\rangle$	0	$\oplus$	$\|\rightarrow\rangle$	1	$\frac{1}{16}$
–	–	–	–	–	0	–	$\|\uparrow\rangle$	0	$\frac{1}{16}$
–	–	–	–	–	1	$\otimes$	$\|\nearrow\rangle$	0	$\frac{1}{8}$

On vérifie que, dans le cas où $b = 0$ (i.e. les lignes autres que 3,5,9,10,14,16), Bob a mesuré un résultat qui pouvait également survenir, avec une probabilité > 0, en l'absence d'Ève. Le protocole proposé à la question 6.1 est donc confirmé.
On voit que E est détectée dans les cas des lignes 5 et 14, non-détectee dans les cas des lignes 3,9,10,16.
Donc

$$\Pr(\text{ E est détectée}) = \frac{1}{32} + \frac{1}{32} = \frac{1}{16}$$

6.3 Supposons que A et B ont "sacrifié" m bits pour tester la présence d'Ève et que Ève a effectivement intercepté ces m qbits. Il s'agit de bits tels que $b = 1$ (selon le protocole de la qu. 6.1).
On calcule :

$$\Pr(b = 1) = \frac{1}{16} + \frac{1}{32} + \frac{1}{32} + \frac{1}{32} + \frac{1}{32} + \frac{1}{16} = \frac{1}{4}$$

Donc

$$\Pr(\text{ E est détectée} \mid b = 1) = \frac{1}{16} : \frac{1}{4} = \frac{1}{4}$$

La probabilité que E soit indétectée apres m vérifications indépendantes (sur des bits tels que $b = 1$) est donc égale à $(\frac{3}{4})^m$, donc la probabilité que E soit *détectée* apres m vérifications indépendantes sur des bits tels que $b = 1$ est :

$$1 - \left(\frac{3}{4}\right)^m .$$

8.1 Les cas où le bit x de A et le bit $1 - y$ de B (i.e. celui inclus dans sa clé) sont différents sont ceux des lignes 5 et 14, soit une fraction $\frac{1}{4}$ des bits tels que $b = 1$. En moyenne il y a *un quart* des positions de bits dont la valeur est différente dans la clé de A et dans la clé de B.
8.2 Par le raisonnement de la qu.5, dans le cas de la ligne 9 (resp. 10), E est certaine que $x = 0$ (resp. $x = 1$). Ces cas représentent $\frac{1}{4}$ des bits de la clé (et il s'agit de bits qui ont bien la même valeur dans C_A et C_B).
9- 9.1 On souhaite calculer

$$\Pr(X_E = x \text{ et } b = 1)$$

Pour cela on reprend les lignes 3,5,9,10,14,16 du tableau de la qu.6.2 et on calcule la valeur de X_E pour chaque ligne :

ligne	x	B_E	μ_E	X_E	p
3	0	$\oplus$	$\|\uparrow\rangle$	0	$\frac{1}{16}$
5	0	$\otimes$	$\|\nearrow\rangle$	1	$\frac{1}{32}$
9	0	$\otimes$	$\|\searrow\rangle$	0	$\frac{1}{32}$
10	1	$\oplus$	$\|\rightarrow\rangle$	1	$\frac{1}{32}$
14	1	$\oplus$	$\|\uparrow\rangle$	0	$\frac{1}{32}$
16	1	$\otimes$	$\|\nearrow\rangle$	1	$\frac{1}{16}$

Eve gagne son pari aux lignes 3,9,10,16 donc

$$\Pr(X_E = x \text{ et } b = 1) = \frac{1}{16} + \frac{1}{32} + \frac{1}{32} + \frac{1}{16} = \frac{3}{16}$$

Comme $\Pr(b = 1) = \frac{1}{4}$, on conclut que :

$$\Pr(X_E = x | b = 1) = \frac{3}{16} : \frac{1}{4} = \frac{3}{4}.$$

9.2 En moyenne, C_E comporte $3n/4$ bits identiques à ceux de la portion de clé $C_A := x_{i_1} \dots x_{i_j} \dots x_{i_n}$.