

EMINES Examen 2026: Information Quantique (Correction)

Zaki Leghtas *

Lundi 9 Février 2026

Questions de cours

Q1. Normalisation de $|\psi_1\rangle = 2|0\rangle + 4i|1\rangle$

La norme de $|\psi_1\rangle$ est :

$$\| |\psi_1\rangle \| = \sqrt{|2|^2 + |4i|^2} = \sqrt{4 + 16} = \sqrt{20} = 2\sqrt{5}.$$

L'état normalisé est donc :

$$|\psi_1\rangle = \frac{1}{\sqrt{5}} |0\rangle + \frac{2i}{\sqrt{5}} |1\rangle.$$

Mesure de \hat{Z} : Les valeurs propres de \hat{Z} sont $+1$ (vecteur propre $|0\rangle$) et -1 (vecteur propre $|1\rangle$). Les probabilités et états post-mesure sont :

$$P(+1) = \left| \frac{1}{\sqrt{5}} \right|^2 = \frac{1}{5}, \quad \text{état projeté : } |0\rangle,$$
$$P(-1) = \left| \frac{2i}{\sqrt{5}} \right|^2 = \frac{4}{5}, \quad \text{état projeté : } |1\rangle.$$

Q2. Valeur moyenne de \hat{X} sur $|\psi_1\rangle$

On calcule d'abord $\hat{X}|\psi_1\rangle$:

$$\hat{X}|\psi_1\rangle = \frac{1}{\sqrt{5}}\hat{X}|0\rangle + \frac{2i}{\sqrt{5}}\hat{X}|1\rangle = \frac{1}{\sqrt{5}}|1\rangle + \frac{2i}{\sqrt{5}}|0\rangle.$$

Puis la valeur moyenne :

$$\langle \hat{X} \rangle = \langle \psi_1 | \hat{X} | \psi_1 \rangle = \frac{1}{\sqrt{5}} \cdot \frac{2i}{\sqrt{5}} + \frac{-2i}{\sqrt{5}} \cdot \frac{1}{\sqrt{5}} = \frac{2i}{5} - \frac{2i}{5} = 0.$$

Q3. Produits $\hat{H}\hat{X}\hat{H}$, $\hat{H}\hat{Y}\hat{H}$, $\hat{H}\hat{Z}\hat{H}$

On rappelle les définitions en notation de Dirac :

$$\hat{H} = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|), \quad \hat{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|.$$

Calcul de $\hat{H}\hat{Z}\hat{H}$:

On commence par $\hat{Z}\hat{H}$ en utilisant $\hat{Z}|0\rangle = |0\rangle$ et $\hat{Z}|1\rangle = -|1\rangle$:

$$\hat{H}\hat{Z}\hat{H} = \frac{1}{\sqrt{2}}(\hat{Z}|0\rangle\langle 0| + \hat{Z}|1\rangle\langle 0| + \hat{Z}|0\rangle\langle 1| - \hat{Z}|1\rangle\langle 1|) = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| - |1\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 1|).$$

*zaki.leghtas@phys.ens.fr

On applique ensuite \hat{H} à gauche, en utilisant la règle $\langle i|j\rangle = \delta_{ij}$:

$$\hat{H}\hat{Z}\hat{H} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|)(|0\rangle\langle 0| - |1\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 1|).$$

En développant et en ne gardant que les termes non nuls ($\langle i|j\rangle = \delta_{ij}$) :

$$\hat{H}\hat{Z}\hat{H} = \frac{1}{2}(2|0\rangle\langle 1| + 2|1\rangle\langle 0|) = |0\rangle\langle 1| + |1\rangle\langle 0| = \hat{X}.$$

$$\hat{H}\hat{Z}\hat{H} = \hat{X}$$

Déduction de $\hat{H}\hat{X}\hat{H}$:

On applique \hat{H} à gauche et à droite du résultat $\hat{H}\hat{Z}\hat{H} = \hat{X}$:

$$\hat{H}(\hat{H}\hat{Z}\hat{H})\hat{H} = \hat{H}\hat{X}\hat{H}.$$

Le membre gauche vaut $(\hat{H}^2)\hat{Z}(\hat{H}^2) = \hat{I}\hat{Z}\hat{I} = \hat{Z}$ car $\hat{H}^2 = \hat{I}$. Donc :

$$\hat{H}\hat{X}\hat{H} = \hat{Z}.$$

$$\hat{H}\hat{X}\hat{H} = \hat{Z}$$

Calcul de $\hat{H}\hat{Y}\hat{H}$ via la relation entre \hat{X} , \hat{Y} , \hat{Z} :

On rappelle les relations $\hat{X}\hat{Y} = i\hat{Z}$, $\hat{Y}\hat{Z} = i\hat{X}$, $\hat{Z}\hat{X} = i\hat{Y}$. Et donc nous avons notamment $\hat{Y} = i\hat{X}\hat{Z}$.

On en déduit $\hat{H}\hat{Y}\hat{H}$ en utilisant les résultats précédents :

$$\hat{H}\hat{Y}\hat{H} = \hat{H}(i\hat{X}\hat{Z})\hat{H} = i(\hat{H}\hat{X}\hat{H})(\hat{H}\hat{Z}\hat{H}) = i\hat{Z}\hat{X} = -\hat{Y}.$$

$$\hat{H}\hat{Y}\hat{H} = -\hat{Y}$$

Bilan : \hat{H} échange $\hat{X} \leftrightarrow \hat{Z}$ et change le signe de \hat{Y} . Ces relations expriment que \hat{H} est une rotation de π autour de l'axe $(\hat{x} + \hat{z})/\sqrt{2}$ sur la sphère de Bloch.

Q4. Montrer que $\hat{H}\hat{T}\hat{H} = \exp(-i\frac{\pi}{8}\hat{X})$ à une phase globale près

Étape 1 — Décomposer \hat{T} sur \hat{I} et \hat{Z} .

On utilise les relations $|0\rangle\langle 0| = \frac{\hat{I} + \hat{Z}}{2}$ et $|1\rangle\langle 1| = \frac{\hat{I} - \hat{Z}}{2}$, de sorte que :

$$\hat{T} = |0\rangle\langle 0| + e^{i\pi/4}|1\rangle\langle 1| = \frac{1 + e^{i\pi/4}}{2}\hat{I} + \frac{1 - e^{i\pi/4}}{2}\hat{Z}.$$

On factorise $e^{i\pi/8}$ à l'aide des identités d'Euler $e^{i\pi/8}(e^{-i\pi/8} + e^{i\pi/8}) = 2\cos\frac{\pi}{8}$ et $e^{i\pi/8}(e^{-i\pi/8} - e^{i\pi/8}) = -2i\sin\frac{\pi}{8}$:

$$\hat{T} = e^{i\pi/8}\left(\cos\frac{\pi}{8}\hat{I} - i\sin\frac{\pi}{8}\hat{Z}\right).$$

On reconnaît la formule $e^{i\theta\hat{A}} = \cos\theta\hat{I} + i\sin\theta\hat{A}$ (avec $\hat{A}^2 = \hat{I}$) :

$$\hat{T} = e^{i\pi/8}\exp\left(-i\frac{\pi}{8}\hat{Z}\right).$$

Étape 2 — Appliquer \hat{H} de part et d'autre.

Pour tout opérateur \hat{A} vérifiant $\hat{A}^2 = \hat{I}$ et toute unitaire $\hat{U} = \hat{U}^\dagger$, la formule $\exp(i\theta\hat{A}) = \cos\theta\hat{I} + i\sin\theta\hat{A}$ donne :

$$\hat{U}e^{i\theta\hat{A}}\hat{U}^\dagger = \cos\theta\hat{I} + i\sin\theta(\hat{U}\hat{A}\hat{U}^\dagger) = e^{i\theta(\hat{U}\hat{A}\hat{U}^\dagger)}.$$

Comme $\hat{H} = \hat{H}^\dagger$, on applique ceci à $\hat{A} = \hat{Z}$, $\hat{U} = \hat{H}$, $\theta = -\frac{\pi}{8}$:

$$\hat{H} \exp\left(-i\frac{\pi}{8}\hat{Z}\right) \hat{H} = \exp\left(-i\frac{\pi}{8} \underbrace{\hat{H}\hat{Z}\hat{H}}_{=\hat{X}}\right) = \exp\left(-i\frac{\pi}{8}\hat{X}\right).$$

Conclusion :

$$\hat{H}\hat{T}\hat{H} = e^{i\pi/8} \hat{H} \exp\left(-i\frac{\pi}{8}\hat{Z}\right) \hat{H} = e^{i\pi/8} \exp\left(-i\frac{\pi}{8}\hat{X}\right).$$

Q5. Intrication de $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

Oui, cet état est intriqué. Supposons par l'absurde :

$$|\psi_2\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle.$$

L'identification impose $ac = 0$, $ad = \frac{1}{\sqrt{2}}$, $bc = \frac{1}{\sqrt{2}}$, $bd = 0$. Or $ac = 0 \Rightarrow a = 0$ ou $c = 0$, ce qui annule respectivement ad ou bc : contradiction. L'état $|\psi_2\rangle = |\Psi^+\rangle$ est donc bien un état de Bell, **intriqué**.

Q6. Calcul de $|\psi_3\rangle = (\hat{Z} \otimes \hat{X}) |\psi_2\rangle$

$$\begin{aligned} (\hat{Z} \otimes \hat{X}) |01\rangle &= (\hat{Z}|0\rangle) \otimes (\hat{X}|1\rangle) = |0\rangle \otimes |0\rangle = |00\rangle, \\ (\hat{Z} \otimes \hat{X}) |10\rangle &= (\hat{Z}|1\rangle) \otimes (\hat{X}|0\rangle) = (-|1\rangle) \otimes |1\rangle = -|11\rangle. \end{aligned}$$

$$|\psi_3\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} = |\Phi^-\rangle.$$

C'est un état de Bell : il est **intriqué** (même argument que Q5).

Q7. Dimension de l'espace et simulation classique

L'espace de Hilbert de n qubits a dimension 2^n .

Un ordinateur classique doit stocker 2^n amplitudes complexes. Pour $n \approx 50$, cela représente $\sim 10^{15}$ nombres complexes (plusieurs pétaoctets). En pratique, la simulation classique d'un état quantique générique devient difficile à partir de $n \approx 50$ qubits.

Q8. Impact de l'algorithme de Shor

L'algorithme de Shor factorise un entier N en temps polynomial $\mathcal{O}((\log N)^3)$ sur un ordinateur quantique, contre un temps sous-exponentiel sur un ordinateur classique. La sécurité du chiffrement RSA repose précisément sur cette difficulté. Un ordinateur quantique suffisamment puissant **compromettrait la quasi-totalité de la cryptographie à clé publique** actuelle (RSA, Diffie-Hellman, courbes elliptiques), mettant en danger les communications sécurisées et les transactions bancaires mondiales.

Mesure d'une observable unitaire

Le circuit (Figure 1) agit sur deux qubits. On note les vecteurs propres de \hat{U} :

$$\hat{U} |u_\pm\rangle = \pm |u_\pm\rangle, \quad |\psi\rangle = \alpha |u_+\rangle + \beta |u_-\rangle.$$

Q9. États $|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle$

$$|\psi_0\rangle = |0\rangle \otimes |\psi\rangle = |0\rangle (\alpha |u_+\rangle + \beta |u_-\rangle).$$

Après \hat{H} sur le qubit 1 :

$$|\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes (\alpha |u_+\rangle + \beta |u_-\rangle) = \frac{1}{\sqrt{2}} (\alpha |0, u_+\rangle + \beta |0, u_-\rangle + \alpha |1, u_+\rangle + \beta |1, u_-\rangle).$$

Après la porte contrôle- \hat{U} (\hat{U} agit sur le qubit 2 si le qubit 1 est dans $|1\rangle$) :

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{2}} (\alpha |0, u_+\rangle + \beta |0, u_-\rangle + \alpha |1\rangle \hat{U} |u_+\rangle + \beta |1\rangle \hat{U} |u_-\rangle) \\ &= \frac{1}{\sqrt{2}} (\alpha |0, u_+\rangle + \beta |0, u_-\rangle + \alpha |1, u_+\rangle - \beta |1, u_-\rangle) \\ &= \frac{1}{\sqrt{2}} (\alpha(|0\rangle + |1\rangle) |u_+\rangle + \beta(|0\rangle - |1\rangle) |u_-\rangle). \end{aligned}$$

Après \hat{H} sur le qubit 1, en utilisant $\hat{H} \frac{|0\rangle \pm |1\rangle}{\sqrt{2}} = |0\rangle$ ou $|1\rangle$:

$$\boxed{|\psi_3\rangle = \alpha |0\rangle |u_+\rangle + \beta |1\rangle |u_-\rangle.}$$

Q10. Résultats de mesure et projections

La mesure de \hat{Z} sur le qubit 1 donne :

Résultat $+1$: prob. $|\alpha|^2$, qubit 2 projeté sur $|u_+\rangle$,

Résultat -1 : prob. $|\beta|^2$, qubit 2 projeté sur $|u_-\rangle$.

Q11. Correspondance avec la mesure de \hat{U}

Une mesure projective de \hat{U} sur $\alpha |u_+\rangle + \beta |u_-\rangle$ donne la valeur propre $+1$ avec probabilité $|\alpha|^2$ (post-état $|u_+\rangle$) et -1 avec probabilité $|\beta|^2$ (post-état $|u_-\rangle$). Le circuit reproduit *exactement* cette statistique : la valeur propre de \hat{U} est transférée sur le qubit ancilla via la porte contrôle- \hat{U} , puis lue par une mesure \hat{Z} . Le qubit cible s'effondre dans le bon état propre de \hat{U} . Ce circuit réalise donc bien une **mesure de l'observable \hat{U}** .

Superdense coding

Q12. États $|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle$ (préparation de la paire de Bell)

$$|\psi_0\rangle = |00\rangle.$$

Après \hat{H} sur le qubit 1 :

$$|\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}.$$

Après CNOT (qubit 1 contrôle qubit 2) :

$$\boxed{|\psi_2\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\Phi^+\rangle.}$$

Q13. $|\psi_2\rangle$ est-il intriqué ?

Oui, $|\psi_2\rangle = |\Phi^+\rangle$ est un état de Bell, maximalement intriqué (même argument que Q5).

Q14. États $|\psi_3\rangle, |\psi_4\rangle, |\psi_5\rangle$ pour les 4 cas (x, y)

Alice applique $\hat{Z}^x \hat{X}^y$ sur son qubit (qubit 1) :

(x, y)	$ \psi_3\rangle$ (après encodage)	$ \psi_4\rangle$ (après CNOT)	$ \psi_5\rangle$ (après H)
$(0, 0)$	$\frac{ 00\rangle + 11\rangle}{\sqrt{2}}$	$\frac{ 00\rangle + 10\rangle}{\sqrt{2}}$	$ 00\rangle$
$(0, 1)$	$\frac{ 10\rangle + 01\rangle}{\sqrt{2}}$	$\frac{ 11\rangle + 01\rangle}{\sqrt{2}}$	$ 01\rangle$
$(1, 0)$	$\frac{ 00\rangle - 11\rangle}{\sqrt{2}}$	$\frac{ 00\rangle - 10\rangle}{\sqrt{2}}$	$ 10\rangle$
$(1, 1)$	$\frac{ 01\rangle - 10\rangle}{\sqrt{2}}$	$\frac{ 01\rangle - 11\rangle}{\sqrt{2}}$	$ 11\rangle$

Détail du cas $(x = 1, y = 1)$: Alice applique $\hat{Z}\hat{X}$ sur le qubit 1 :

$$\hat{Z}\hat{X}|0\rangle = \hat{Z}|1\rangle = -|1\rangle, \quad \hat{Z}\hat{X}|1\rangle = \hat{Z}|0\rangle = |0\rangle.$$

$$|\psi_3\rangle = \frac{-|1\rangle|0\rangle + |0\rangle|1\rangle}{\sqrt{2}} = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

Après CNOT ($|10\rangle \rightarrow |11\rangle, |01\rangle \rightarrow |01\rangle$) :

$$|\psi_4\rangle = \frac{|01\rangle - |11\rangle}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes |1\rangle.$$

Après \hat{H} sur qubit 1 : $H \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |1\rangle$, donc $|\psi_5\rangle = |11\rangle$.

Q15. Récupération de (x, y) par mesure \hat{Z}

Dans tous les cas, $|\psi_5\rangle = |xy\rangle$ (état de la base computationnelle). La mesure de \hat{Z} donne :

$$\text{qubit 1 : } +1 \Leftrightarrow x = 0, \quad -1 \Leftrightarrow x = 1,$$

$$\text{qubit 2 : } +1 \Leftrightarrow y = 0, \quad -1 \Leftrightarrow y = 1.$$

On obtient donc les deux bits (x, y) avec **certitude**, en n'ayant transmis qu'un seul qubit. C'est la magie du *superdense coding* : l'intrication préalablement partagée permet de doubler la capacité de transmission.