ENSEIRB-MATMECA
Option second semestre, 2013/2014

Information Quantique

Corrigé de l'examen du 19 Mai 2014

Notation : la note finale est
min(20, note-ex1+note-ex2+note-ex3).

Exercice 1 (/15 pts)

Intrication, corrélation.

1- $|\Phi_1\rangle$ est intriqué (vu en cours).
$|\Phi_2\rangle := \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Donc $|\Phi_2\rangle$ est factorisable.
$\sqrt{3}\,|\Phi_3\rangle = (a\,|0\rangle + b\,|1\rangle) \otimes (c\,|0\rangle + d\,|1\rangle)$ ssi :

$$ac = 1,\ \ ad = 1,\ bc = 0,\ \ bd = 1$$

Mais $bc = 0 \Rightarrow (b = 0$ ou $c = 0) \Rightarrow bd = 0$ ou $ac = 0$ ce qui est incompatible avec $bd = ac = 1$. Donc $\sqrt{3}\,|\Phi_3\rangle$ est intriqué. Mais l' ensemble des vecteurs factorisables est clos par produit par les scalaires (par bilinéarité de $\otimes$). Donc l'ensemble des vecteurs intriqués est clos par produit par les scalaires non-nuls. On en conclut que $|\Phi_3\rangle$ est intriqué.
$\sqrt{5}\,|\Phi_4\rangle := (a\,|0\rangle + b\,|1\rangle) \otimes (c\,|0\rangle + d\,|1\rangle)$ ssi :

$$ac = 1,\ \ ad = 0,\ bc = 0,\ \ bd = 2$$

Mais $ad = 0 \Rightarrow (ac = 0$ ou $bd = 0)$, ce qui est impossible. Donc $|\Phi_4\rangle$ est intriqué.
2- Supposons que le vecteur $|\Phi\rangle = \sum_{(i,j)\in[1,2]\times[1,2]} t_{i,j}\,|i\rangle\otimes|j\rangle$ est factorisable : $|\Phi\rangle = u \otimes v$ avec $u = u_0\,|0\rangle + u_1\,|1\rangle$, $v = v_0\,|0\rangle + v_1\,|1\rangle$.
Alors

$$\begin{vmatrix} t_{0,0} & t_{0,1} \\ t_{1,0} & t_{1,1} \end{vmatrix} = u_0 v_0 u_1 v_1 - u_1 v_0 u_0 v_1 = 0.$$

Donc le rang de la matrice $T := (t_{i,j})_{(i,j)\in[1,2]\times[1,2]}$ vaut 0 ou 1.
Supposons que le rang de T vaut 0 ou 1.
Si $rg(T) = 0$ alors $|\Phi\rangle = 0 = 0 \otimes 0$.

Si $rg(T) = 1$ alors, choisissons un indice $i_0 \in \{0,1\}$ tel que $(t_{i_0,0}, t_{i_0,1}) \neq (0,0)$ et notons $\lambda \in \mathbb{C}$ un complexe tel que

$$(t_{1-i_0,0}, t_{1-i_0,1}) = \lambda(t_{i_0,0}, t_{i_0,1}).$$

Posons

$$u_{i_0} := 1, u_{1-i_0} := \lambda, v_0 := t_{i_0,0}, v_1 := t_{i_0,1}.$$

On a bien, pour tous $(i,j) \in \{0.1\} \times \{0,1\}$

$$t_{i,j} = u_i v_j.$$

Donc

$$|\Phi\rangle = (u_0 |0\rangle + u_1 |1\rangle) \otimes (v_0 |0\rangle + v_1 |1\rangle).$$

Les déterminants associés aux vecteurs $|\Phi_0\rangle, \ldots, |\Phi_4\rangle$ valent :

$$\frac{1}{2}\begin{vmatrix}1 & 0\\ 0 & 1\end{vmatrix} = \frac{1}{2}, \quad \frac{1}{4}\begin{vmatrix}1 & 1\\ 1 & 1\end{vmatrix} = 0, \quad \frac{1}{3}\begin{vmatrix}1 & 1\\ 0 & 1\end{vmatrix} = \frac{1}{3}, \quad \frac{1}{5}\begin{vmatrix}1 & 0\\ 0 & 2\end{vmatrix} = \frac{2}{5}.$$

On retrouve ainsi que seul $|\Phi_2\rangle$ est factorisable et que les autres états sont intriqués.
3- Supposons que $|\Phi\rangle$ est factorisable :

$$|\Phi\rangle = |u\rangle \otimes |v\rangle .$$

Alors,

$$(U_0 \otimes U_1) |\Phi\rangle = (U_0 |u\rangle) \otimes (U_1 |v\rangle),$$

donc $(U_0 \otimes U_1) |\Phi\rangle$ est factorisable.
Supposons que $(U_0 \otimes U_1) |\Phi\rangle$ est factorisable. Alors, par le raisonnement ci-dessus, appliqué aux transformations unitaires U_0^{-1}, U_1^{-1}, on obtient que

$$(U_0^{-1} \otimes U_1^{-1})(U_0 \otimes U_1) |\Phi\rangle$$

est factorisable, i.e. que $|\Phi\rangle$ est factorisable.
4- Soient $|\Phi\rangle$ et $|\Psi\rangle$ factorisables et de norme 1. Alors

$$|\Phi\rangle = |u\rangle \otimes |v\rangle , \quad |\Psi\rangle = \left|u'\right\rangle \otimes \left|v'\right\rangle .$$

On sait que $\langle u|u\rangle \cdot \langle v|v\rangle = 1$ On peut donc réécrire

$$|\Phi\rangle = |u_1\rangle \otimes |v_1\rangle$$

où $|u_1\rangle = \frac{1}{\sqrt{\langle u|u\rangle}}|u\rangle, |v_1\rangle = \frac{1}{\sqrt{\langle v|v\rangle}}|v\rangle$ sont maintenant, des vecteurs de norme 1. De même, on peut réécrire

$$|\Psi\rangle = \left|u_1'\right\rangle \otimes \left|v_1'\right\rangle$$

où les vecteurs $|u_1'\rangle, |v_1'\rangle$ sont de norme 1. Il existe des transformations unitaires de déterminant 1, U_0, U_1 telles que :

$$U_0|u_1\rangle = \left|u_1'\right\rangle, \;\; U_1|v_1\rangle = \left|v_1'\right\rangle.$$

Donc

$$\begin{aligned}(U_0 \otimes U_1)|\Phi\rangle &= (U_0 \otimes U_1)(|u_1\rangle \otimes |v_1\rangle) \\ &= \left|u_1'\right\rangle \otimes \left|v_1'\right\rangle \\ &= |\Psi\rangle.\end{aligned}$$

5- Soient U_0, U_1 des transformation unitaires, de déterminant 1, telles que

$$(U_0 \otimes U_1)|\Phi_1\rangle = |\Phi_4\rangle.$$

Notons, pour $j \in \{0,1\}, U_j = \begin{pmatrix} \alpha_j & -\overline{\beta_j} \\ \beta_j & \overline{\alpha_j} \end{pmatrix}$. On aurait alors :

$$\frac{1}{\sqrt{2}}[(\alpha_0\alpha_1+\overline{\beta_0\beta_1})|00\rangle+(\alpha_0\beta_1-\overline{\beta_0}\overline{\alpha_1})|01\rangle+(\beta_0\alpha_1-\overline{\alpha_0}\overline{\beta_1})|10\rangle+(\beta_0\beta_1+\overline{\alpha_0\alpha_1})|11\rangle] = |\Phi_4\rangle$$

Ce qui entrainerait que :

$$\alpha_0\alpha_1 + \overline{\beta_0\beta_1} = \frac{\sqrt{2}}{\sqrt{5}}, \;\; \beta_0\beta_1 + \overline{\alpha_0\alpha_1}) = \frac{2\sqrt{2}}{\sqrt{5}}$$

donc que

$$\frac{\sqrt{2}}{\sqrt{5}} = \frac{2\sqrt{2}}{\sqrt{5}}$$

qui est clairement faux. On en conclut que U_0, U_1 n'existent pas.
6- 6.1 Supposons que $|\Phi\rangle$ est un état factorisable :

$$|\Phi\rangle = |u\rangle \otimes |v\rangle. \tag{1}$$

Notons $X_0 := X, X_1 := Y$. Pour tout $\eta \in \mathbb{C}$ notons $\mathcal{B}_{j,\eta} := \mathrm{Ker}(X_j - \eta\mathrm{I})$, $\mathcal{H}_{1,\eta} := \mathrm{Ker}(\mathrm{I} \otimes X_1 - \eta\mathrm{I})$, $\mathcal{H}_{0,\eta} := \mathrm{Ker}(X_0 \otimes \mathrm{I} - \eta\mathrm{I})$, $\mathrm{pr}_{\mathcal{B}_{j,\eta}}$ la projection orthogonale de $\mathcal{B}_j$ sur son sous-espace $\mathcal{B}_{j,\eta}$ et $\mathrm{pr}_{\mathcal{H},j,\eta}$ la projection orthogonale

de $\mathcal{H}$ sur son sous-espace $\mathcal{H}_{j,\eta}$.
On sait que

$$\Pr(\{\mathcal{X}=\lambda \text{ et } \mathcal{Y}=\mu\}) = \|\mathrm{pr}_{\mathcal{H},0,\lambda} \circ \mathrm{pr}_{\mathcal{H},1,\mu} |\Phi\rangle \|^2$$

(comme dans l'exercice 22, Q1, du polycopié). La décomposition (1) de $|\Phi\rangle$ entraine que :

$$\mathrm{pr}_{\mathcal{H},1,\mu} |\Phi\rangle = |u\rangle \otimes (\mathrm{pr}_{\mathcal{B}_1,\mu} |v\rangle)$$
$$\mathrm{pr}_{\mathcal{H},0,\lambda}(\mathrm{pr}_{\mathcal{H},1,\mu} |\Phi\rangle) = (\mathrm{pr}_{\mathcal{B}_0,\lambda} |u\rangle) \otimes (\mathrm{pr}_{\mathcal{B}_1,\mu} |v\rangle)$$

donc

$$\begin{aligned} \Pr(\{\mathcal{X}=\lambda \text{ et } \mathcal{Y}=\mu\}) &= \|(\mathrm{pr}_{\mathcal{B}_0,\lambda} |u\rangle) \otimes (\mathrm{pr}_{\mathcal{B}_1,\mu} |v\rangle)\|^2 \\ &= \|\mathrm{pr}_{\mathcal{B}_0,\lambda} |u\rangle \|^2 \cdot \|\mathrm{pr}_{\mathcal{B}_1,\mu} |v\rangle \|^2 \qquad (2) \end{aligned}$$

$$\begin{aligned} \Pr(\{\mathcal{X}=\lambda\}) &= \|\mathrm{pr}_{\mathcal{H},0,\lambda}(|u\rangle \otimes |v\rangle)\|^2 \\ &= \|(\mathrm{pr}_{\mathcal{B}_0,\lambda} |u\rangle) \otimes |v\rangle \|^2 \\ &= \|\mathrm{pr}_{\mathcal{B}_0,\lambda} |u\rangle \|^2. \qquad (3) \end{aligned}$$

car $\langle v|v\rangle = 1$.

$$\begin{aligned} \Pr(\{\mathcal{Y}=\mu\}) &= \|\mathrm{pr}_{\mathcal{H},1,\mu}(|u\rangle \otimes |v\rangle)\|^2 \\ &= \| |u\rangle \otimes (\mathrm{pr}_{\mathcal{B}_1,\mu} |v\rangle)\|^2 \\ &= \|\mathrm{pr}_{\mathcal{B}_1,\mu} |v\rangle \|^2. \qquad (4) \end{aligned}$$

car $\langle u|u\rangle = 1$.
Il découle de (2)(3)(4) que,

$$\Pr(\{\mathcal{X}=\lambda \text{ et } \mathcal{Y}=\mu\}) = \Pr(\{\mathcal{X}=\lambda\}) \cdot \Pr(\{\mathcal{Y}=\mu\}).$$

Comme cette égalité est vérifiée pour tous les nombres complexes λ, μ, les variables aléatoires $\mathcal{X}, \mathcal{Y}$ sont indépendantes.
6.2 De façon générale, si $\mathcal{X}, \mathcal{Y}$ sont des v.a. indépendantes alors leur covariance est nulle. Donc, lorsque $|\Phi\rangle$ est factorisé, $\mathrm{Covar}(\mathcal{X}, \mathcal{Y}) = 0$.
7- 7.1

$$\begin{aligned} \mathbb{E}(\mathcal{X}) &= \sum_{\lambda \in \{+1,-1\}} \Pr(\mathcal{X}=\lambda) \cdot \lambda \\ &= \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot (-1) \\ &= 0 \end{aligned}$$

De même $\mathbb{E}(\mathcal{Y}) = 0$.

$$\begin{aligned}\mathbb{E}(|\mathcal{X}|^2) &= \sum_{\lambda\in\{+1,-1\}} \Pr(\mathcal{X}=\lambda)\cdot|\lambda|^2 \\ &= \frac{1}{2}\cdot 1^2 + \frac{1}{2}\cdot(-1)^2 \\ &= 1\end{aligned}$$

De même $\mathbb{E}(|\mathcal{Y}|^2) = 1$.
7.2

$$\begin{aligned}\mathbb{E}(\overline{\mathcal{X}}\cdot\mathcal{Y}) &= \sum_{\lambda\in\{+1,-1\},\mu\in\{-1,+1\}} \Pr(\mathcal{X}=\overline{\lambda},\mathcal{Y}=\mu)\cdot\overline{\lambda}\mu \\ &= \frac{1}{2}\cdot 1^2 + 0\cdot(1)(-1) + 0\cdot(-1)(1)\frac{1}{2}\cdot(-1)(-1) \\ &= 1.\end{aligned}$$

Donc $\mathrm{Var}(\mathcal{X}) = 1, \mathrm{Var}(\mathcal{Y}) = 1, \mathrm{Covar}(\mathcal{X},\mathcal{Y}) = 1$ et la corrélation de $\mathcal{X},\mathcal{Y}$ vaut 1.
8- Par des calculs similaires :

$$\mathbb{E}(\mathcal{X}) = \mathbb{E}(\mathcal{Y}) = 0,\ \ \mathbb{E}(|\mathcal{X}|^2) = \mathbb{E}(|\mathcal{Y}|^2) = 1,\ \ \mathbb{E}(\overline{\mathcal{X}}\cdot\mathcal{Y}) = 1$$

d'où il découle que la corrélation de $\mathcal{X},\mathcal{Y}$ vaut 1.
9- Comme, d'après la question 7, dans l'état $|\Phi_1\rangle$ les observables $\mathcal{X},\mathcal{Y}$ ont une covariance non-nulle, d'après la question 6, l'état $|\Phi_1\rangle$ n'est pas factorisable i.e. est intriqué.
De même, comme d'après la question 8, dans l'état $|\Phi_4\rangle$ les observables $\mathcal{X},\mathcal{Y}$ ont une covariance non-nulle, l'état $|\Phi_4\rangle$ est intriqué.

Exercice 2(/10 pts)

Borne de Tsirelson.

1- Supposons que $U : \mathcal{H} \to \mathcal{H}$ est unitaire. Alors, pour tout $u \in \mathbb{H}$ tel que $\|u\| = 1$ on a $\|Uu\| = 1 \leq 1\cdot\|u\|$, donc $\|U\| \leq 1$. Par ailleurs, il existe un vecteur unitaire u tel que $\|Uu\| = 1$. Donc $\sup\{\|Mu\| \mid u \in E, \|u\| = 1\} = 1$ i.e. $\|U\| = 1$.
2- Ces opérateurs sont unitaires, donc ils ont tous une norme qui vaut 1.
3- Soient M, N sont des application linéaires de E dans E.

On vérifie que, pour tout $u \in E$, $\|Nu\| \leq \|N\| \cdot \|u\|$. Pour tout $u \in E$ tel que $\|u\| = 1$:

$$\begin{aligned} \|M \cdot Nu\| &\leq \|M\| \cdot \|Nu\| \\ &\leq \|M\| \cdot \|N\| \cdot \|u\|. \end{aligned}$$

et

$$\begin{aligned} \|(M+N)u\| &= \|Mu + Nu\| \\ &\leq \|Mu\| + \|Nu\| \\ &\leq \|M\|\|u\| + \|N\|\|u\| \\ &= (\|M\| + \|N\|) \cdot \|u\| \end{aligned}$$

Donc

$$\|M \cdot N\| \leq \|M\| \cdot \|N\| \text{ et } \|(M+N)\| \leq \|M\| + \|N\|.$$

4-

$$4G_\psi = \langle\psi| A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1) |\psi\rangle$$

Sachant que pour tous vecteurs $|u\rangle, |v\rangle$,

$$|\langle u|v\rangle| \leq \| |u\rangle \| \cdot \| |v\rangle \|$$

et que $\| |\Psi\rangle \| = 1$, on a :

$$\begin{aligned} 4G_\psi &\leq \| |\psi\rangle \| \cdot \|A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1) |\psi\rangle \| \\ &\leq \|A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1) |\psi\rangle \| \end{aligned}$$

Utilisons maintenant les proriétés de la norme des opérateurs vue à la Q3 :

$$\begin{aligned} 4G_\psi = & \|[A_0 \otimes (B_0 + B_1) |\psi\rangle] + [A_1 \otimes (B_0 - B_1) |\psi\rangle]\| \\ \leq & \|A_0 \otimes (B_0 + B_1) |\psi\rangle \| + \|A_1 \otimes (B_0 - B_1) |\psi\rangle \| \\ = & \|(A_0 \otimes \mathrm{I})(\mathrm{I} \otimes (B_0 + B_1)) |\psi\rangle \| + \|(A_1 \otimes \mathrm{I})(\mathrm{I} \otimes (B_0 - B_1)) |\psi\rangle \| \\ = & \|(\mathrm{I} \otimes (B_0 + B_1)) |\psi\rangle \| + \|(\mathrm{I} \otimes (B_0 - B_1)) |\psi\rangle \| \qquad \text{car } (A_j \otimes \mathrm{I}) \text{ est unitaire} \\ = & \| |\Phi_0\rangle + |\Phi_1\rangle \| + \| |\Phi_0\rangle - |\Phi_1\rangle \|. \end{aligned}$$

5- Comme les B_j sont unitaires, les $\mathrm{I} \otimes B_j$ sont aussi unitaires, donc les vecteurs Φ_j sont unitaires.
Pour deux vecteurs quelconques $|u\rangle, |v\rangle$ on a :

$$\langle u+v|u+v\rangle = \langle u|u\rangle + \langle v|v\rangle + 2\mathcal{R}(\langle u|v\rangle).$$

Donc, pour les vecteurs unitaires $|\Phi_0\rangle, |\Phi_1\rangle$ et tout $\varepsilon \in \{1, -1\}$ on a :

$$\langle \Phi_0 + \varepsilon\Phi_1 | \Phi_0 + \varepsilon\Phi_1 \rangle = 2 + 2\varepsilon\mathcal{R}(\langle \Phi_0 | \Phi_1 \rangle),$$

d'où :

$$\| \, |\Phi_0\rangle + |\Phi_1\rangle \, \| + \| \, |\Phi_0\rangle - |\Phi_1\rangle \, \| \leq \sqrt{2 + 2\mathcal{R}(\langle \Phi_0 | \Phi_1 \rangle)} + \sqrt{2 - 2\mathcal{R}(\langle \Phi_0 | \Phi_1 \rangle)}$$

6- La fonction $f : x \mapsto \sqrt{2+2x} + \sqrt{2-2x}$, est dérivable sur $]-1, +1[$, et

$$f'(x) = \frac{\sqrt{2-2x} - \sqrt{2+2x}}{4 - x^2}.$$

Comme f' est positive sur $]-1, 0]$ et négative sur $[0, 1[$, f atteint un maximum au point 0 et ce maximum vaut $f(0) = 2\sqrt{2}$.
7-
7.1 En combinant les résultats des questions 4,5 et 6, on obtient que $4G_\psi \leq 2\sqrt{2}$. donc

$$G_\psi \leq \frac{\sqrt{2}}{2}$$

7.2 On a vu en cours que la valeur $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ permet d'atteindre une espérance de gain exactement égale à $\frac{\sqrt{2}}{2}$. On peut conclure que ce choix de vecteur partagé pour Anne et Benoit *maximise* leur gain moyen (dans l'ensemble de toutes les stratégies décrites au début de l'exercice).

Exercice 3(/15 pts)

Transformation de Fourier quantique.

1-

$$\omega^N = (e^{\frac{2i\pi}{N}})^N = e^{2i\pi} = 1.$$

2- Soit m un nombre entier tel que $0 < m < N$.Posons :

$$C(N, m) := (\omega^m)^N = e^{\frac{2i\pi m}{N}}.$$

2.1 Comme la période de la fonction $x \mapsto e^{2i\pi x}$ vaut 1, $C(N, m) = 1$ ssi $\frac{m}{N}$ est une multiple entier de 1, i.e. un entier, ce qui n'est pas vrai. Donc $(\omega^m)^N \neq 1$.
2.2 En utilisant la factorisation : $X^N - 1 = (X-1)(\sum_{j=0}^{N-1} X^j)$ on obtient :

$$(\omega^m)^N - 1 = (\omega^m - 1)(\sum_{j=0}^{N-1} (\omega^m)^j).$$

Par Q1 on sait que le membre gauche est nul. Par Q2 on sait que $(\omega^m - 1) \neq 0$. Il s'en suit que

$$\sum_{j=0}^{N-1} (\omega^m)^j = 0.$$

2.3- Soient $0 \leq j \leq \ell \leq N-1$.
Sachant que la base $(e_j)_{j\in[0,N-1]}$ est orthonormée, on obtient :

$$\langle \mathcal{F}(e_j) | \mathcal{F}(e_\ell) \rangle = \frac{1}{N} \sum_{k=0}^{N-1} (\omega^{k(\ell-j)}) \tag{5}$$

D'après Q2.2, si $j < \ell$ alors le membre droit de (5) est nul. Si $j = \ell$, le membre droit de (5) vaut $\frac{1}{N}\sum_{k=0}^{N-1} 1 = 1$. La base $(\mathcal{F}(e_j))_{j\in[0,N-1]}$ est donc orthonormée, ce qui montre que $\mathcal{F}$ est unitaire.
3- Comme le produit tensoriel de deux e.v. E, F sur un corps K est un espace de dimension $\dim(E) \cdot \dim(F)$ sur K, l'espace $\mathcal{B}^{\otimes n}$ est une espace vectoriel de dimension 2^n sur $\mathbb{C}$. On le munit d'une forme sequilinéaire hermitienne positive non-dégénérée en posant

$$\langle b_1 \dots b_j \dots b_n | c_1 \dots c_j \dots c_n \rangle = \prod_{j\in[1,n]} \langle b_j | c_j \rangle \tag{6}$$

(voir polycopié, chapitre 9).
4- Appliquons la définition (6) aux vecteurs $|k\rangle, |\ell\rangle$:

$$\langle k|\ell\rangle \quad = \quad \langle k_1 \dots k_j \dots k_n | \ell_1 \dots \ell_j \dots \ell_n \rangle = \prod_{j\in[1,n]} \langle k_j | \ell_j \rangle$$

Si $k = \ell$ alors le membre droit ci-dessus vaut $\prod_{j\in[1,n]} \langle k_j | k_j \rangle = 1$ (car les vecteurs k_j sont de norme 1.
Si $k \neq \ell$ alors le membre droit ci-dessus vaut $\prod_{j\in[1,n]} \langle k_j | \ell_j \rangle$ qui comporte au moins un terme $\langle k_j | \ell_j \rangle$ où $k_j \neq \ell_j$ ce qui entraine que $\langle k_j | \ell_j \rangle = 0 = \langle k | \ell \rangle$. La famille $(|j\rangle)_{j\in[0,N-1]}$ est donc orthonormée. Comme elle a la cardinalité 2^n, c'est bien une base orthonormée de $\mathcal{B}^{\otimes n}$.
5- On calcule :

$$R_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad R_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}; \quad R_2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}; \quad R_3 = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{pmatrix};$$

6- Considérons l'égalité :

$$\sum_{k=0}^{N-1} (\omega^{kj}) \, |k\rangle = \bigotimes_{\ell=1}^{n} (|0\rangle + e^{2i\pi \frac{j}{2^\ell}} \, |1\rangle) \tag{7}$$

Développons le produit tensoriel du membre droit en combinaison linéaire des vecteurs de la base $(|k\rangle)_{k\in[0,N-1]}$. Le coefficient de $|k\rangle$ vaut :

$$\begin{aligned}\prod_{k_\ell=1} e^{2i\pi\frac{j}{2^\ell}} \cdot \prod_{k_\ell=0} e^{2i\pi j0} &= \prod_{\ell=1}^{n} e^{2i\pi j\frac{k_\ell}{2^\ell}} \\ &= e^{2i\pi j\sum_{\ell=1}^{n} k_\ell 2^{-\ell}} \\ &= e^{\frac{2i\pi j}{N}\sum_{\ell=1}^{n} k_\ell 2^{n-\ell}} \\ &= e^{\frac{2i\pi jk}{N}} \\ &= \omega^{jk} = \omega^{kj}\end{aligned}$$

qui est aussi le coefficient de $|k\rangle$ dans le membre gauche. L'égalité (7) est donc établie. En multipliant les deux membres de cette égalité par $\frac{1}{\sqrt{2^n}}$ on obtient :

$$\mathcal{F}\,|j\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{\ell=1}^{n} \left(|0\rangle + e^{2i\pi\frac{j}{2^\ell}}\,|1\rangle\right) \tag{8}$$

7- Soit

$$j = \sum_{k=1}^{n} j_k 2^{n-k}$$

Alors

$$\begin{aligned}e^{2i\pi\frac{j}{2^\ell}} &= e^{2i\pi\sum_{k=1}^{n} j_k 2^{n-k-\ell}} \\ &= e^{2i\pi\sum_{k=n-\ell+1}^{n} j_k 2^{n-k-\ell}} \\ &= e^{2i\pi 0.j_{n-\ell+1}j_{n-\ell+2}\cdots j_n}.\end{aligned}$$

8- En remplaçant, dans le membre droit de (8), le terme $e^{2i\pi\frac{j}{2^\ell}}$ par l'expression obtenue à la question 7, on obtient

$$\mathcal{F}\,|j\rangle = \frac{1}{2^{n/2}}(|0\rangle + e^{2i\pi\,0.j_n}\,|1\rangle)\otimes(|0\rangle + e^{2i\pi\,0.j_{n-1}j_n}\,|1\rangle)\otimes\ldots\otimes(|0\rangle + e^{2i\pi\,0.j_1 j_2\ldots j_n}\,|1\rangle)$$

9- Si $j_1 = 0$: $H\,|j_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi 0.j_1}\,|1\rangle)$
Si $j_1 = 1$: $H\,|j_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi}\,|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi 0.j_1}\,|1\rangle)$.
10- Par la question 9 :

$$|j_1 j_2\rangle \overset{H\otimes \mathrm{I}}{\mapsto} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2i\pi 0.j_1}\,|1\rangle\right)\otimes|j_2\rangle$$

Si $j_2 = 0$,

$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2i\pi 0.j_1}\ |1\rangle\right) \otimes |0\rangle \quad \overset{cR_2}{\mapsto} \quad \left(|0\rangle + e^{2i\pi 0.j_1}\ |1\rangle\right) \otimes |0\rangle$$
$$= \quad \left(|0\rangle + e^{2i\pi 0.j_1 j_2}\ |1\rangle\right) \otimes |j_2\rangle\,.$$

Si $j_2 = 1$, alors l'action de cR_2 consiste a multiplier le premier qbit par $i = e^{2i\pi 0.0 j_2}$, donc, dans ce cas aussi

$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2i\pi 0.j_1}\ |1\rangle\right) \otimes |j_2\rangle \overset{cR_2}{\mapsto} \left(|0\rangle + e^{2i\pi 0.j_1 j_2}\ |1\rangle\right) \otimes |j_2\rangle\,.$$

11- De façon générale, l'action de la porte cR_ℓ consiste à multiplier le coefficient du vecteur $|1\rangle$ (dans l'état du premier qbit) par $e^{\frac{2i\pi}{2^\ell}} = e^{2i\pi\, 0.b_1 b_2 \ldots j_\ell}$ (avec $b_k = 0$), ce qui revient à ajouter le bit j_ℓ, en position ℓ après la virgule, dans le nombre binaire qui multiplie $2i\pi$ en exposant de e. L'application successive des portes $cR_3 ... cR_n$ conduit donc à

$$|j_1 j_2 j_3 \ldots j_n\rangle \to \left(|0\rangle + e^{2i\pi\, 0.j_1 j_2 \ldots j_n}\,|1\rangle\right) \otimes |j_2 j_3 ... j_n\rangle\,.$$

Remarquons que l'ordre d'application de ces $(n-1)$ portes est indifférent.
12- La succession de portes agissant sur le deuxième qubit $|j_2\rangle$ s'exprime par la formule trouvée à la question 11, appliquée à l'entier $n-1$ (au lieu de n) et où l'on renomme les indices $1, 2, \ldots, n-1$ en $2, \ldots, n$. On obtient ainsi :

$$|j_2 j_3 \ldots j_n\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2i\pi\, 0.j_2 \ldots j_n}\,|1\rangle\right) \otimes |j_3 ... j_n\rangle$$

13- Une fois que tous les qubits ont été traités, l'état obtenu est :

$$\frac{1}{2^{n/2}}(|0\rangle + e^{2i\pi\, 0.j_1 j_2 \ldots j_n}\,|1\rangle) \otimes (|0\rangle + e^{2i\pi\, 0.j_2 \ldots j_n}\,|1\rangle) \otimes ... \otimes (|0\rangle + e^{2i\pi\, 0.j_n}\,|1\rangle)$$

i.e. que le facteur le plus à gauche est celui de Q11, le suivant (de gauche à droite) est celui de Q12, etc... et le plus à droite est $(|0\rangle + e^{2i\pi\, 0.j_n}\,|1\rangle)$.
Pour obtenir $\mathcal{F}\,|j\rangle$, il reste à "inverser" l'ordre des qbits, i.e. appliquer la transformation unitaire $\hat{\mathsf{INV}}_n$ où $\mathsf{INV}_n : [1, n] \to [1, n]$ est l'application $m \mapsto n + 1 - m$. On vérifie que la permutation INV_n est le produit de $\lfloor n/2 \rfloor$ portes SWAP (classiques). Le circuit SWAP à n qbits est le circuit quantique correspondant.